ARTICLE 29 - DATA PROTECTION WORKING PARTY

10557/02/EN final
WP 54

FIFTH ANNUAL REPORT

ON THE SITUATION REGARDING THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND PRIVACY IN THE EUROPEAN UNION AND IN THIRD COUNTRIES

COVERING THE YEAR 2000

PART II

Adopted on 6th March 2002

FIFTH ANNUAL REPORT ON THE SITUATION REGARDING THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND PRIVACY IN THE COMMUNITY AND IN THIRD COUNTRIES COVERING THE YEAR 2000

PART II

ARTICLE 29 DATA PROTECTION WORKING PARTY'S ACTIVITIES DURING THE YEAR 2000 AND PICTURE OF THE MAIN DEVELOPMENTS IN THE EUROPEAN UNION ON PRIVACY AND DATA PROTECTION, AS WELL AS PRINCIPAL DEVELOPMENTS IN THIRD COUNTRIES AND OTHER DEVELOPMENTS AT INTERNATIONAL LEVEL

1.4. Main developments in the Member States concerning the following issues:

A. Legislative measures adopted under the first pillar (this is excluding Directives 95/46/EC and 97/66/EC)

B. Changes made under the second and third pillar

C. Major case law

D. Specific issues

E. Website

for the following countries:

INTRODUCTION TO PART II

This is the fifth annual report covering the year 2000 of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data[1], hereinafter called the Article 29 Data Protection Working Party. The report is addressed to the Commission, the European Parliament, the Council as well as to the public at large. The Article 29 Data Protection Working Party is the independent European Union advisory body on data protection and privacy[2] . Its report is intended to give an overview on the situation of the protection of individuals concerning the processing of personal data in the European Union and in third countries[3].

The general Data Protection Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter "the Directive") was adopted on 24 October 1995 and required implementation not later than three years after this date (24 October 1998)[4] . The specific Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector, adopted by the European Parliament and the Council on 15 December 1997, aligned the date for its transposition with that of the General Directive.

The first report explained the composition and tasks of the Article 29 Data Protection Working Party and covered the main facts observed in 1996 in the field of data protection . The second report covered the year 1997 and essentially followed the structure of the first report, in order to facilitate analysis of developments. The third annual report continued this tradition: it first presented an overview of main developments in the European Union, both in the Member States and at Community level and addressed then the work of the Council of Europe. The report further informed about the main developments in third countries and other developments at international level. In the fourth report Article 29 Data Protection Working Party's activities were presented more prominently in a separate chapter and more emphasis was placed on questions related to the European Union.

This fifth report will, for the first time, be published in the form of a glossy brochure. On this occasion, the first part of this report presents the members of the Article 29 Data Protection Working Party and its Secretariat from its beginning until 2000. It explains the mission of the Article 29 Data Protection Working Party, its rules of procedure and gives an overview of the main issues addressed in 2000. A glossary has been introduced to assist readers in finding the information they are seeking in the documents adopted.

---

1 Established by Article 29 of Directive 95/46/EC. Its tasks are laid down in Article 30 and in Article 14 (3) of Directive 97/66/EC. See part I, page 24.

2 See Article 29 (1) second sentence of Directive 95/46/EC.

3 See Article 30 paragraph 6 of Directive 95/46/EC.

4 This date is different from the date of entry into force: Since the Directive does not specify the date of its entry into force, it came into force on the 20th day following the day of its publication (see Article 254 (1) of the Treaty).

Main issues addressed during the year 2000 at Community level concern first of all transfers of personal data to third countries, in particular to the United States of America under the "safe harbor" agreement; as well as Internet, telecommunications and electronic commerce and finally the implementation of Directive 95/46/EC.

In 2000, the Article 29 Data Protection Working Party met six times. It was dealing with 53 items on its agenda and treated about 66 documents in view of the preparation of its opinions, recommendations and working documents.

The Article 29 Data Protection Working Party's opinions and recommendations were transmitted to the Commission and to the Article 31 Committee and where appropriate to the presidents of the Council, the European Parliament and others.

The Secretariat of the Article 29 Data Protection Working Party is provided by the

European Commission
Directorate General Internal Market
Data protection unit

The documents adopted by the Article 29 Data Protection Working Party are available at this unit's web page on the Website "Europa" of the European Commission at:

http://europa.eu.int/comm/privacy

1. DEVELOPMENTS IN THE EUROPEAN UNION ON PRIVACY AND DATA PROTECTION

1.1. Directive 95/46/EC

1.1.1. Implementation into national law

Austria

The Directive has been implemented by the Data Protection Act 2000. The "Bundesgesetz über den Schutz personenbezogener Daten" entered into force on 1.01.2000 (Datenschutzgesetz 2000, BGBl. I Nr. 165/1999 of 17.08.1999 http://www.bka.gv.at/datenschutz/dsg2000e.pdf)

Because of its federal structure and the separation of responsibilities between the federation and the "Länder", the directive can only be implemented at the level of the federation in the sectors which fall under its jurisprudence responsibility, which is the case for the whole area of automated data processing. Data protection concerning manually structured data application falls under the responsibility of the "Länder", as far as data are processed for the purpose of the "Länder"; i.e. for those aspects the "Länder" have to implement the Directive. In fact, 7 out of 9 "Länder" have fulfilled their obligation and adopted regional data protection laws.

In 2000 the ordinance on standard processing operations has been adopted implementing the data protection law 2000 (and thereby as well directive 95/46/EC) and entered into force on 1st July 2000 (Verordnung des Bundeskanzlers über Standard- und Musteranwendungen nach dem Datenschutzgesetz 2000 (Standard- und Muster-Verordnung 2000 – StMV), Federal Law Gazette II Nr. 201/2000, about exceptions from notification). In this ordinance some "routine" data processing operations whose maximum content is precisely fixed by this ordinance are excepted from the notification obligation to the data processing registry held by the data protection commission (so-called "standard applications"). For certain other data applications this ordinance foresees a simplified notification obligation (so-called "model applications").

Belgium

The implementation law will enter into force on 1 September 2001 (Belgian law of December 8, 1992 on privacy protection in relation to the processing of personal data, as modified by the law of December 11, 1998, implementing Directive95/46/EC.
http://www.law.kuleuven.ac.be/icri/papers/legislation/privacy/engels/

Following a public consultation that took place in December 1999, the elaboration of the Royal Decree implementing the law took place in the course of year 2000. The Royal Decree was adopted on 13 February 2001 (O.J. 13 March 2001), and provides

for the entry into force of the law 6 months after its publication, i.e. on 1 September 2001.

Denmark

The Act on Processing of Personal Data (Act No. 429 of 31 May 2000) was adopted on 31 May 2000 and entered into force on 1 July 2000. The act implements Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data http://www.datatilsynet.dk/eng/index.html.

The act substitutes The Public Authorities' Registers Act and The Private Registers Act.

Finland

The Directive of the European Parliament, and of the Council, on the protection of individuals with regard to the processing of personal data and on the free movement of such data (95/46/EC) was enacted in Finland with the Personal Data Act (523/1999), which entered into force on 1 June 1999 http://www.tietosuoja.fi.

The Act was revised on 1 December 2000, when provisions on the Commission's decision-making, as well as how binding these decisions are, in matters concerning the transfer of personal data to countries outside the Union under the Data Protection Directive were incorporated in it.

Protection of privacy has been a basic right in Finland since 1 August 1995. Under the Finnish Constitution, protection of personal data is regulated by a separate act.

France

In the spring of 2000, the Government asked the National Commission for Informatics and Freedom (CNIL), as well as the Advisory Committee on Human Rights (Commission consultative des droits de l'homme), for an opinion on a preliminary draft law concerning the protection of individuals with regard to the processing of personal data and amending Law No 78-17 of 6 January 1978 on data processing, files and freedoms. The draft law was adopted by the Council of Ministers on 18 July 2001. Having been submitted to the National Assembly, this draft is scheduled to be examined at the beginning of January 2002. (http://www.assemblee-nat.fr/dossiers/cnil.asp)

Germany

In the course of modernizing German data protection law, the Federal Government is following a two-phase approach.

The first one was in substance directed towards implementing the Directive. On 14 June 2000 the Federal Government (Bundeskabinett) agreed on a draft law amending the German data protection law (BDSG). The Chamber of State representatives (Bundesrat) made comments to this draft law on 29 September 2000. On 13 October 2000 the draft law amending the German data protection law (BDSG) and other laws was submitted by the Federal Government to the Bundestag (BT-Drs. 14/4329). Discussions in the various committees of the Federal Parliament (Bundestag) started in 2000 and were concluded by the law modifying the Federal Data Protection Act and other Acts (Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze) as of 22 May 2001, Federal Law Gazette Vol. I, p. 904.

Subsequent to this novellization, the second phase, which has been started already, is aiming at a fundamental reform of data protection law. An important step in this direction has been made by handing over the expert report on the modernisation of data protection law ("Modernisierung des Datenschutzrechts") on 12 November 2001 to the Federal Ministry of the Interior.
http://www.bfd.bund.de/information/bdsg_hinweis.html

Greece

The data protection law has been implemented by Law 2472 on the Protection of individuals with regard to the processing of personal data. This law has been adopted on 10 April 1997 and entered into force the same day. The English version is available at http://www.dpa.gr/Documents/Eng/2472engl_all.doc

Ireland

Current position : A draft heads of a bill (general outline of proposed legislation) was presented to Government in July 1998.

Next steps : A draft Bill has been prepared which has to be approved by Government and submitted to Parliament. The government's legislative programme indicates that publication is expected by early 2002.

Italy

Directive 95/46/EC was transposed into Italian law by Act no. 675 of 31.12.1996 – the Data Protection Act.

Throughout 2000 the activities continued which aimed at streamlining domestic law in accordance with the principles set out in Act no. 675/1996. In particular, based on the experience gathered in the past few years in implementing the Act, the focus of attention was on checking completeness and effectiveness of the regulatory policies adopted in the Data Protection Act and therefore on identifying those areas where more detailed, specific provisions were required. This analysis led to postponing – to the 31st of December, 2001 - the deadline by which Government was enabled to

adopt the legislative measures required in order to complete the reference regulatory framework applying to personal data processing. The relevant enabling statute was passed in March 2001 and will be addressed in greater detail in next year's annual report.

The aforementioned statute also provides that all the provisions concerning the protection of individuals and other entities with regard to the processing of personal data and all the related measures will have to be included into a consolidated text by the end of 2002, in order to facilitate consultation and operational coordination.

Great importance should be attached to the regulatory activities carried out by the Garante in the year 2000, when the authority used the atypical regulatory tools provided for by the Data Protection Authority in order to set out the conditions under which the processing of personal data for historical and statistical purposes is lawful. This exercise was completed in 2001 with the cooperation of the relevant stakeholders. Codes of conduct and professional practice were drafted and agreed upon in the sectors mentioned above.

Luxembourg

The draft Luxembourg law transposing Directive 95/46/EC was presented to the Parliament on 7 December 2000.

The document is available at www.chd.lu under *PORTAIL DOCUMENTAIRE, Recherche d'archives, Recherche avancée, Dossier Parlementaire n° 4735*.

Four opinions have been presented to date by the:

- Chamber of Civil Servants and Public Employees (*Chambre des Fonctionnaires et Employés Publics*)
- State Public Prosecutor (*Procureur Général d'Etat*)
- Chamber of Labour (*Chambre de Travail*)
- Chamber of Private Sector Employees (*Chambre des Employés Privés*)

Netherlands

The main instrument adopted during this period is the new Dutch Data Protection Act. This act bears the date of 6 July 2000[5] and implements Directive 95/46/EC into Dutch law.

This new law replaces the act of 28 December 1988, but there is great degree of continuity from one to the other act. A number of differences deserve to be mentioned:

[5] Wet van 6 juli 2001, houdende regels inzake de bescherming van persoonsgegevens (Wet Bescherming Persoonsgegevens), Staatsblad 2000 302. An unofficial English translation of this act is available on the website of the Dutch Data Protection Authority: www.cbpweb.nl.

- The scope of application is now defined in the same terms as those of the European Directive. While the previous law applied to the so-called "registration of persons", with an emphasis basically on the keeping of files concerning several persons, the new act refers to "processing", that is defined as in article 2 of the Directive.
- The new law does not make any difference between public sector and private sector processing operations in general terms.
- Transparency becomes the cornerstone of the law. In particular, the act emphasises the need to provide adequate and timely information to the data subject so that he can take informed decisions concerning his own personal data.
- A new right to oppose is included in the same terms as defined in the Directive.
- The new act contains a whole chapter dealing with the issue of trans-border data flows to countries outside the European Union. In principle data may only be sent to countries with an adequate level of protection or in the cases where one of the exceptions enumerated in the act applies. The Minister of Justice may, after having being advised by the Data Protection Authority, grant a permit for a specific transfer or set of transfers if the controller adduces sufficient guarantees. This can be done in particular through contractual clauses.
- Under the new act the Dutch Data Protection Authority (up to now called Registratiekamer in Dutch) gets a new name, College Bescherming Persoonsgegevens, and some new competencies. In particular, and in addition to the penal provisions contained in the act, the Data Protection Authority gets new powers concerning sanctions and may in some cases impose fines or administrative measures of constraint. The Dutch Data Protection Authority does not have any competencies concerning freedom of information issues.

Portugal

The Directive was transposed into national law in 1998, by the Data Protection Act (Law 67/98, of 26 October).

The Portuguese Data Protection Authority gave Opinions during 2000, regarding matters directly connected to the European Union activity, such as: the data protection adequacy of Hungarian laws, Swiss laws and the Safe Harbor principles; the joint secretariat for the supervisory bodies of Europol, Schengen and Customs; and the personal data processing by the Institutions and bodies of the Community and the freedom of circulation of those data.

Sweden

Directive 95/46/EC was implemented in Sweden by the entry into force of the Personal Data Act (1998:204) on 24 October 1998. http://www.datainspektionen.se/in_english/default.asp?content=/in_english/legislation/data.shtml

Secondary legislation, *i.e.* the Personal Data Ordinance (1998:1191), came into force on the same day. The previous data protection act in Sweden, the Data Act (1973:289), has continued to apply provisionally to processing operations initiated before 24 October 1998. Since 1 October 2001 however, the new legislation is fully applicable as regards automated processing of personal data. All manual processing will fall under the new legislation from 1 October 2007.

In principal, the Personal Data Act applies to processing of personal data in all sectors. However, it exempts processing of personal data to the extent that such processing has been specifically regulated in another statute or enactment. Specific acts have been adopted for personal data processing in the police sector and the health and medical sector etc. (f.ex. Act on records of medical data (1998:543), Act on health care records (1998:544), Act on records of convicted persons (1998:620), Act on records of suspected persons (1998:621), Police Data Act (1998:622)).

Spain

The most significant event was the coming into force, on 14 January 2000, of Organic Law No. 15/1999 on the protection of personal data.
(https://www.agenciaprotecciondatos.org/datd1.htm)

United Kingdom

In the year 2000 the Data Protection Act 1998 came into force. http://www.hmso.gov.uk/acts/acts1998/19980029.htm
This legislation ensured that the United Kingdom had implemented the provisions of Directive 95/46/EC. Implementation enhanced the framework of rights and responsibilities that had previously been available under the Data Protection Act 1984. Secondary legislation was also introduced to give effect to the provisions of the Act.

1.1.2. Infringement proceedings

The European Commission decided in December 1999 to take France, Luxembourg, the Netherlands, Germany and Ireland to the European Court of Justice for failure to notify all the measures necessary to implement Directive 95/46/EC. This step represents the third formal stage of formal infringement proceedings under Article 226 of the EC Treaty. In 2001 the Netherlands and Germany have notified and the Commission decided to close the cases against them.

1.2. Directive 97/66/EC

1.2.1. Implementation into national law

Austria

Austria implemented Directive 97/66/EC by means of the Telecommunications Act, BGBl. I No 100/1997.

Belgium

The provisions of Directive 97/66/EC have been integrated into Belgian law by way of amendments to already existing legislation.

Articles 78-79 of the Consumer Protection Act of 14/07/91 have been amended in order to provide for the regulation of unsolicited calls for the purposes of direct marketing. The new provisions have entered into force on 01/10/99 ((*Moniteur Belge* (hereinafter M.B.) 23/06/99)). Article 9 of the Royal Decree on telecommunications of 22/06/98 has been amended on 08/07/99, in order to integrate the provisions of the Directive regarding the Calling Line Identification system. The amendments entered into force on 01/09/99 (M.B. 01/09/99). A Royal Decree on directories was adopted on 14/09/99. It entered into force on 18/09/99 (M.B. 18/09/99). It provides for certain conditions to be fulfilled before publication of personal data in directories may take place.

The Article 105 of the law of 21 March 1991 on Public Economic Companies has been completely amended in order to implement the provision of Directive 97/66/EC related to the handling and preservation of traffic data by telecom operators and telecom service providers. It entered into force on 21 December 1999 (M.B. 21.12.99).

Denmark

The directive was transposed into national law in Denmark by the Act on Competitive Conditions and Consumer Interest in the Telecommunications Market (Act No. 418 of 31 May 2000), by Executive Order on Number Information Databases (Executive Order No. 665 of 6 July 2000) and by Executive Order on the Provision of Telecommunications Networks and Telecommunications Services (Executive Order No. 569 of 22 June 2000 now No. 1169 of 15 December 2000).

Finland

The Directive concerning the processing of personal data and the protection of privacy in the telecommunications sector (97/66/EC) was enacted in Finland with the Act on the Protection of Privacy and Data Security in Telecommunications (565/1999), which entered into force on 1 July 1999.

When the Eureopan Union launched a revision of the Telecommunications Privacy Directive, action was simultaneously taken in Finland to assess the need for revising national legislation.

France

In January 2000, and again in June 2000, the Government successively informed the CNIL about a preliminary draft law and a draft decree intended to supplement internal legislation. The legislative measures were adopted under Ordinance No 2001-670 of 25 July 2001. This text makes direct marketing by automatic calling system or fax subject to the prior consent of the persons concerned being obtained.

Germany

Telecommunications Data Protection Ordinance of 18 Dec. 00 (in power as of 21 December 2001) -Telekommunikationsdatenschutzverordnung (TDSV).

Greece

The Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector was transposed into national law in Greece with the Act 2670/98 on the protection of personal data in the telecommunications sector.

Ireland

During 2000 the Directive was not transposed into Irish law, but it is hoped to be transposed by early 2002.

Italy

Directive 97/66/EC was implemented in Italy by way of legislative decree no. 171/1998.
A few amendments to said decree are required in order to bring it fully into line with the directive – with particular regard to emergency calls and alternative billing modalities, which were the subject of an infringement proceeding that was opened against Italy. These amendments will be made by way of the provisions issued on the basis of the enabling statute referred to above.

Luxembourg

Up to now no text for transposition of the directive has been produced.

Netherlands

The most relevant piece of legislation containing sectoral rules on this issue is the Telecommunications Act of October, 19, 1998[6]. This law partly implements Directive 97/66/EC into Dutch law but a number of issues still need to be dealt with in secondary legislation.

Portugal

The Directive was transposed into national law in 1998 by the Act regulating the personal data protection and the privacy in the telecommunications sector – Law 69/98 of 28 October.

Article 9 of the Directive: the Data Protection Authority pronounced on the situations of exceptions regarding the elimination of the presentation of calling line identification, appreciating the circumstances of adequacy, necessity and proportionality, provided in national law. It was considered that whenever a called subscriber asks for the use of the exception, in case of malicious calls, the service provider shall balance the rights of the calling user and the rights of the called subscriber, by requesting for instance more information about the frequency and nature of the calls. A simple questionnaire would allow to decide for the adequacy and proportionality of revealing the identification of the calling user.

The Portuguese Data Protection Authority organised, in November 2000, a Colloquium on "Privacy and Electronic Commerce", which had a major participation of companies operating in this field, as well as of university students, and also of the French Data Protection Authority (CNIL).

With great coverage from the press, in this colloquium were presented academic studies and real experiences about the situation of e-commerce in Portugal and the privacy policies adopted by the enterprises on-line. The data protection principles and the intervention of the supervisory authority, along with the role of the ISP's in the security of the information circulating in the Internet, the digital signature, and the rights of the consumers were other themes discussed, that raised interest and debate among the participants.

Spain

The most significant event was the coming into force, on 14 January 2000, of Organic Law No. 15/1999 on the protection of personal data.

6 Wet van 19 oktober 1998, houdende regels inzake de telecommunicatie (Telecommunicatiewet), Staatsblad 1998 610.

Sweden

Directive 97/66/EC was implemented into Swedish law in 1998 by amendments in the Telecommunications Act (1993:597) and the Telecommunications Ordinance (1997:399) mainly. These amendments came into force on 1 July 1999. Article 4.1 of the Directive, regarding security measures, was implemented by section 31 of the Personal Data Act, which came into force on 24 October 1998. Confidentiality of communications (article 5 of the Directive) is, in addition to provisions in the Telecommunications Act, also regulated by chapter 4, section 8, of the Penal Code (1962:700). Article 12 of the Directive, regarding unsolicited calls for direct marketing purposes, was implemented by an amendment of the Marketing Practices Act (1995:450), which came into force on 1 May 2000.

United Kingdom

On the 1st March 2000 the Telecommunications (Data Protection and Privacy) Regulations 1999 came into force. These gave effect to Directive 97/66/EC (with the exception of the provisions of Article 5). The Regulations provided a statutory framework for the UK's Telephone and Fax Preference Services

1.2.2. Infringement proceedings

All Member States but three have notified measures implementing the specific data protection Directive (97/66/EC). The proceedings against Belgium, Denmark, Greece and the United Kingdom were terminated in 2000. The Commission is studying the measures of which it has been appraised. But in July 2000 the Commission decided to refer its case against Ireland for failure to notify full transposal measures to the Court. It had taken the same decision in relation to France and Luxembourg in 1999. The Advocate-General presented his conclusions in the case against France (C-151/00) on 26 October. Regarding Article 5 of the directive, which was due to be transposed by 24 October 2000, letters of formal notice were sent to France, Ireland, Italy, Luxembourg and the United Kingdom for failure to notify the Commission of implementing measures. Eleven Member States had notified implementing measures by the end of 2000.

1.3. Issues addressed by the Article 29 Data Protection Working Party

1.3.1. Transfer of data to third countries – USA: Safe Harbor Principles

The Article 29 Data Protection Working Party expressed its final view on this issue in 2000[7]. While it recognised the commercial and economic importance of the arrangement in its last opinions thereon, it highlighted certain issues of concern which it had regarding the principles.

These issues of concern included the need to clarify that the safe harbour principles do not displace Member State law, the possibility of organisations being members of the safe harbour while not being subject to FTC type jurisdiction, the breadth of the exceptions to the safe harbour standards, the issue of onward transfers taking place in the U.S. to a third party not subscribing to the safe harbour and finally, the weaknesses within proposed enforcement mechanisms. The Article 29 Data Protection Working Party urged that improvements be made in these areas as it was of the belief that a better standard in terms of data protection was achievable.

1.3.2. Standard contractual clauses

Although most will recall the year 2000 as the year of the discussion on the U.S. Safe Harbor, it was in this year that the Article 29 Data Protection Working Party set up the foundations for the standard contractual clauses to be approved by the Commission the year after.

Indeed, model contracts had been the subject of certain debate before, in particular after the submission of two draft model contracts by the International Chamber of Commerce and the Confederation of British Industry. These discussions revealed, on the one hand, that Industry's proposals were far away from the expectations of the Article 29 Data Protection Working Party and, on the other hand, that Industry's representatives did not seem prepared to meet most of the concerns. As a matter of fact, no new drafts were presented, so that the discussions about both initiatives were not followed up.

Being this the situation, the Safe Harbor's discussions revealed the necessity of a contractual solution being readily available, in particular, for those sectors of activity likely to be excluded from the scope of the Draft Commission Decision on the adequacy of the Safe Harbor (U.S. Financial and Telecommunications sectors). The final Opinion of the Article 29 Data Protection Working Party on this subject made this concern explicit in one of its conclusions.

---

7 WP 31 (5019/00) Opinion 3/2000 on the EU/US dialogue concerning the 'Safe Harbour' arrangement, adopted on 16.3.2000.
WP 32 (CA07/434/00/EN) Opinion 4/2000 on the level of protection provided by the 'Safe Harbour Principles', adopted on 16.5.2000.
See also chapter 3.3 United States of America, page 68

Therefore, the Commission Services submitted to the Article 29 Data Protection Working Party a first Draft Commission Decision on standard contractual clauses in July. In the meeting of September, the plenary decided to extend the mandate of the contractual clauses` subgroup to discuss with the Commission this new initiative. From this moment on, the subgroup met several times with the Commission[8] as a sort of drafting group paving the way for the discussions in the plenary. These discussions took place in October and in an extraordinary meeting in November which was convoked by the President precisely to put this dossier forward. The activities of the Article 29 Data Protection Working Party on this subject in the year 2000 finished with a letter of the Chairman to the members of the Article 31 Committee[9] summarising the preliminary conclusions of the discussions held.

The Article 29 Data Protection Working Party's input to the Draft Commission Decision on standard contractual clauses must be highlighted. The contributions of the Article 29 Data Protection Working Party's members based on their practical experience with model contracts at national level were considered extremely helpful by the Commission and played a crucial role in the Article 31 Committee's further unanimous approval to the Commission Decision 2001/497/EC.

1.3.3. Internet, telecommunications and electronic commerce

A. Internet

In 2000 the Article 29 Data Protection Working Party undertook to produce a comprehensive document[10] relating to privacy on the Internet which combined an analysis of the Directives applying to this area together with the opinions already adopted by the Article 29 Data Protection Working Party. The document was the result of intensive preparatory work on this area by the Internet Task Force (ITF) created by the Article 29 Data Protection Working Party in 1999.

The document had a number of objectives. Primarily it sought to raise awareness on the privacy issues that arise for individuals through their use of the Internet and to offer guidance for business and individuals on the application of the directives[11] in this field. Furthermore it was hoped that the document might raise some new issues which requiring individual work could be addressed at a later stage.

As the Internet is an open network with vast quantities of personal data processed over it, more by accident than by design, many of its technical characteristics can lead to the invasion of the privacy of its users. The use of browser chattering, cookies and

---

8 The representatives of the Austrian, British, Dutch, French and Spanish members of the Article 29 Data Protection Working Party attended these meetings. The drafts were submitted to the European Commission in view of a finding in the sense of article 26(4) of Directive 95/46/EC. The Commission consulted the Article 29 Data Protection Working Party. The Article 29 Data Protection Working Party had set up a subgroup on standard contractual clauses which prepared the plenary discussion and findings.

9 Established by Article 31 of Directive 95/46/EC and composed of representatives of the Member States.

10 WP 37 (5063/00) Working Document on Privacy on the Internet- An integrated EU Approach to On-Line Data Protection, adopted on 21.11.2000.

11 Directive 95/46/EC and Directive 97/66/EC.

hyperlinks provide the potential for invisible profiling of every individual internet user.

This Working Document addresses the fact that personal data processing on the internet has to be considered in the light of Directive 95/46/EC and in some cases Directive 97/66/EC.

It explains the technical features of email and the privacy risks associated therewith. The discussion covers such issues as retention of 'deleted' emails, problems associated with the use of webmail accounts and the possibilities created for commercial operators by use of sniffing and spamming. It then offers concrete guidance on the legality of such activities under the directives. The point is also clearly made that right to secrecy and anonymity of correspondence should be respected with regard to email as much as to traditional mail.

Concerning the problem of 'spamming' the Article 29 Data Protection Working Party makes certain recommendations on how the data subject should be protected in view of the fact that on the basis of current European Union legislation the Member States can choose between an 'opt in' and an 'opt out' procedure. At the same time, the Article 29 Data Protection Working Party fully supports the Commission proposal to harmonise this situation by introducing 'opt in'.

With regard to surfing the Internet, the paper outlines in detail the personal data collected in the technical processes involved in Internet use. It highlights the invisible privacy risks inherent in Internet use, both through collection of email addresses and analysis of the users' behaviour on-line. It also discusses the possibility created by new software of compiling comprehensive files on Internet users.

Through the application of data protection principles to the process of Internet use a number of issues are highlighted - the importance of having an accurate, concise and highly visible privacy policy on each site, of anonymising data if it is not immediately deleted, of ensuring finality of processing and of ensuring that the speed of data flows on the Internet does not lead to a neglect of data protection rules. Specifically the Article 29 Data Protection Working Party supports the idea that surfing behaviour data should be afforded the same level of data protection as content.

The applicability of data privacy principles to data made publicly available on the web (e.g. chat rooms, directories) is discussed and the Article 29 Data Protection Working Party stresses the point that data protection rules continue to apply to data made public.

The role of data protection rules in e-commerce is also explained. It is pointed out that for a transaction to be completed on-line it may be necessary that a large amount of personal data is shared between numerous actors. Furthermore the actions of the consumer can be meticulously monitored in an e-commerce transaction in a way not possible in the physical world. The application of data protection rules by e-commerce actors would however considerably reduce such risks.

Under Article 7 (b) of the Directive is it permissible for an individual's data to be processed where this is necessary for the conclusion of a transaction. This provides

the basis for those who trade on the web to process personal data without explicit consent. However in this context the Article 29 Data Protection Working Party points out that the processing of any data over and above that which is strictly necessary for the conclusion of the transaction or for a purpose other than the conclusion of a transaction would not be lawful if based only on this provision.

Finally the Article 29 Data Protection Working Party recommend the use of Privacy Enhancing Technologies (PET's) as a technical solution to many data protection problems in this field. Such technology can be relied on to preserve anonymity or pseudonymity and prevent data being used for a purpose other than that for which it was originally collected and hence guard the purpose limitation principle. Furthermore they suggest the introduction of a European standard for privacy labels to ensure that such labels can be relied upon.

In conclusion, the Article 29 Data Protection Working Party offers some general recommendations on the subject. It points out that there is an obligation upon both the public and private sector to raise awareness amongst consumers both of the risk of their privacy rights being violated on line and what they can do to prevent this. They urge Member States to ensure a coherent application of data protection rules and those involved in the development of software to keep data protection rules in mind when designing their product.

B. Telecommunications

Early in 2000, the Article 29 Data Protection Working Party welcomed the proposed review of Directive 97/66/EC[12] and expressed its wish to have an input into any revision thereof. It highlighted the fact that any new Directive had to be drafted in light of Directive 95/46/EC and in particular, it welcomed the proposed re-examination of terminology used in Directive 97/66/EC and recommended that the increasing role of software in the telecommunications field should be taken into account in any review.

Later in the year, the Article 29 Data Protection Working Party gave a detailed opinion on the proposed revision of the directive[13]. While they welcomed the effort made to clarify terminology used in the Directive, they also called for a clarification of certain points and an explanation as to why certain changes had been made.

With regard to the content of the draft directive, they again stressed that confidentiality of communications must be the general rule, with few exceptions allowed. Further, they recommended a thorough review of the rules on traffic data and location data and stressed that any protection granted by the original directive should be maintained, if not strengthened. Considering the exceptions contained in the Directive, they warned against broadening those allowed under Directive 95/46/EC.

---

12 WP 29 (5009/00) Opinion 2/2000 concerning the general review of the telecommunications legal framework, adopted on 3.2.2000.

13 WP36 (5042/00) Opinion 7/2000 on the European Commission Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, adopted on 2.11.2000.

Further, the Article 29 Data Protection Working Party recommended that a specific reference be included in the directive placing an obligation on developers of technology to design their equipment with data protection principles in mind.

C. E-Commerce

In 2000 the Article 29 Data Protection Working Party continued to address new data protection issues posed by developments in the area of electronic commerce. Specifically, the areas of 'spamming'[14] and electronic public directories [15] were considered in detail. The Article 29 Data Protection Working Party highlighted the problems which these new technologies can create for data subjects. In the case of unsolicited email - the collection of email addresses without consent and the cost of connection time associated with these mails, in the case of electronic directories - the possibilities of invasion of privacy created by the availability of a reverse search facility.

The Article 29 Data Protection Working Party reiterated the fact that data protection legislation applies to processing of personal data undertaken in the context of e-commerce and expressed its opinion that the introduction of the proposed e-commerce Directive would not change the law as regards data protection principles, but would rather supplement it.

With regard to 'spamming', they drew an important distinction between situations where email addresses are procured directly from the addressee and where addresses are collected from a public space such as Internet sites without the knowledge of the individuals, and explained how the relevant Directives[16] could be used to protect data subjects rights in both cases.

In relation to electronic directories, the Article 29 Data Protection Working Party were of the opinion that reverse searches were useful and should not be prohibited as such. However they were of the view that data controllers should have to inform data subjects about the new purposes for which their data could be used once it was assimilated into the Directories and obtain their consent. On this issue the Article 29 Data Protection Working Party therefore fully supported the European Commission's proposal for a draft directive concerning the processing of personal data and the protection of privacy in the electronic communications sector which takes into account the various usage possibilities of, in particular, electronic public directories.

---

14 WP 28 (5007/00) Opinion 1/2000 on certain data protection aspects of electronic commerce, adopted on 3.2.2000.

15 WP 33 (5058/00) Opinion 5/2000 on the Use of Public Directories for Reverse or Multi-criteria Searching Services, adopted on 13.7.2000.

16 Directive 95/46/EC and draft Electronic Commerce Directive.

1.3.4. Implementation of Directive 95/46/EC

The Article 29 Data Protection Working Party drew attention to the fact that a large number of Member States were late in implementing the directive and highlighted the negative consequences of this delay[17]. Further the Article 29 Data Protection Working Party expressed its support for the infringement proceedings that the Commission, as guardian of the European Communities Treaties, were bringing as a result. Where Member States fail to implement the Directive, there is no legislative framework on which the national Supervisory Authority established under Article 28 of the Directive can base its decisions and develop its advisory role. Ultimately, the citizens of that Member State lose out. Business has no legal certainty and the benefits of the Internal Market are not availed of.

1.3.5. Genetic data

On 26 June 2000, the President of the United States of America and the Prime Minister of the United Kingdom made a joint public presentation of the completion of the DNA blueprint achieved by a joint venture of public and private researchers. This announcement got considerable media attention.

The Article 29 Data Protection Working Party in a short Opinion approved on 13 July[18] welcomed this scientific achievement while recalling that the abuse of genetic knowledge can raise legitimate concerns about the privacy of individuals.

1.3.6. Codes of conduct

1) FEDMA

During the year 2000, the FEDMA subgroup of the Article 29 Data Protection Working Party continued its discussions with FEDMA's representatives and reported to the plenary in February and October where new versions of the Code were submitted by FEDMA to the Article 29 Data Protection Working Party. Considerable progress was made and quite a lot of technical and substantial issues of the code were agreed.

One of these difficult issues was the question of the lawfulness of the processing of sensitive data for direct marketing purposes where opinion even within the Article 29 Data Protection Working Party seemed to differ. FEDMA requested and the Article 29 Data Protection Working Party adopted unanimously an official position on this issue which was delivered as a letter to FEDMA at the end of the year.

---

17 WP 30 (5139/99) Recommendation 1/2000 on the Implementation of Directive 95/46/EC, adopted on 3.2.2000.

18 Opinion 6/2000 on the Human Genome and Privacy, adopted on 3.2.2000.

2) IATA

The work on the International Air Transport Association's (IATA) "Recommended Practice 1774 - Protection of privacy and transborder data flows of personal data used in international air transport of passengers and cargo (RP 1774)" continued in 2000. Several meetings took place between the subgroup representing the Article 29 Data Protection Working Party and IATA. It became clear that this recommended practice has another objective than Community codes of conduct within the meaning of Article 27 of directive 95/46/EC. Nevertheless, IATA tried to take over as much as possible from the Article 29 Data Protection Working Party's suggestions to bring RP 1774 in line with the directive and to strengthen the protection of privacy and personal data in international air transport. IATA adopted in December 2000 the revised version of RP 1774 on which the Article 29 Data Protection Working Party gave its final view[19].

1.3.7. European Union Charter on Fundamental Rights

In its Recommendation 4/99 on the inclusion of the fundamental right to data protection in the European catalogue of fundamental rights, the Article 29 Data Protection Working Party supported the European Council's initiative to draw up an European Union Charter of fundamental rights and recommended the inclusion of the fundamental right to privacy and data protection in this Charter. The Article 29 Data Protection Working Party announced also that it was prepared to help in the drawing-up of the Charter. This request was realised by the input made through the Chairman of the Article 29 Data Protection Working Party, Prof. Rodotá who became a member of the drafting Convention of the Charter[20].

The European Union Charter of Fundamental Rights has been officially proclaimed by the European Parliament, the Council and the Commission on the 7 of December 2000 at the occasion of the intergovernmental conference on the Nice Treaty[21].

In addition to article 7 that relates to the respect for private and family life, the Charter contains article 8 which ensures specifically the protection of personal data. This provision is drafted as follows:

---

19 WP 49 (5032/01) Working Document on IATA Recommended Practice 1774 Protection for privacy and transborder data flows of personal data used in international air transport of passengers and of cargo, adopted on 13 September 2001.

20 When the European Council met in Tampere, Finland, on 15 and 16 October 1999, it laid down in precise terms how the Charter of fundamental rights in the European Union should be drawn up. The European Council entrusted this task to an ad hoc body called "Convention", composed of representatives of the heads of state and government, the President of the European Commission, Members of the European Parliament and national Members of Parliament. The Convention was chaired by Mr. Roman Herzog, former President of the Federal Republic of Germany.

21 Published in Official Journal 2000/C 364/1.

"1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority. "

1.4. Main developments in the Member States concerning the following issues:

A. Legislative measures adopted under the first pillar (this is excluding Directives 95/46/EC and 97/66/EC

B. Changes made under the second and third pillar

C. Major case law

D. Specific issues

E. Website

for the following countries:

Austria

A. Legislative measures adopted under the first pillar

In the area of the "Länder", competent for jurisdiction in certain matters, various laws with particular relevance for data protection have been prepared and respectively adopted.

In some "Länder" new laws have been adopted with regard to Youth Welfare laws, regulating in particular the notifications made by individuals where there is suspicion of neglect, mistreatment or sexual abuse of minors and the collection of personal data related thereto.

Furthermore the Vienna law on archives has been adopted, by which legal regulations have been created to ensure the archiving of the Land Vienna's archiving material and the access to the Land's and the City of Vienna's archiving material for citizens and scientific research.

B. Changes made under the second and third pillar

For the first time, a law on military competencies has been adopted where certain tasks to be fulfilled in the framework of military defence of the "Länder" are anchored and which sets standards for the competencies of military authorities and organs including the use of personal data for military affairs. By this law special instruments

for legal protection have been created in the area of the "Länder's" military defence, in particular the office of the legal protection officer has been established.

By the adoption of a new law on security police law the competencies of security police have been extended to the so-called "enlarged danger investigation" (in the case of tasks linked to a situation with concrete indication on the existence of danger involving security police). The creation of an institution of a controlling legal protection officer (Rechtsschutzbeauftragter) accompanying the activities of the investigating authorities ensures special legal protection in this sensitive area.

C. Major case law

None.

D. Specific issues

In the year 2000 the Data Protection Commission has executed a particularly important control procedure - the examination of the so-called electronic criminal police information system (Elektronisches Kriminalpolizeiliches Informationssystem - EKIS) used by the Ministry of the Interior to support the criminal police work of the Austrian security authorities. The reason for this examination was the following: a former police officer had published a book where the frequent occurrence of unjustified questioning of the EKIS was reported, in particular concerning politicians and journalists.

In the framework of this system questions in relation to examination procedures were raised, in particular, as to which data applications are exempted from the notification obligation for the purpose of the fight against crime. According to § 17 para 3 of the Data Protection Act 2000 (Datenschutzgesetz, DSG 2000) data applications are exempted from the notification obligation, amongst others, for the purpose of protection of constitutional institutions of the Austrian republic respectively the prevention, stopping or prosecution of crimes, only, as long as this is necessary for the realisation of the purpose of data application. In all the other cases the notification obligation remains. In particular for data applications whose content is already determined by law, exemptions from the registration obligation may hardly be maintained because of the prevailing secrecy obligation. As a consequence it has been recommended to the Ministry of the Interior (as operator of the joint information system) to examine the "EKIS" data as to the new legal situation and catch up with the necessary notifications without delay.

Furthermore, the Data Protection Commission defended the view that user protocols which can, from a technical viewpoint, only be evaluated by sequential research are not sufficient neither in respect of data protection nor to guarantee the individual's right of information. User protocols of the EKIS have to be organised in a way that it can easily be determined without employing disproportionate means, whether data concerning a certain individual have been questioned and who did the questioning and for what purpose.

Likewise, the reinforcement of the system in case of possible questioning abuse has been recommended, in particular, to promote the development of special support software (f.i. routine evaluation programmes) which should soon be put into practice.

The Ministry of the Interior has declared its readiness, to take the necessary steps to follow this recommendation and has already implemented some of its items.

For quite some time preparatory work has been done in Austria to introduce a smart card for social security. Every person subject to insurance should receive such a card. This smart card shall replace the present health insurance certificate. At the end of 2000 the federal government decided that this smart card should be used also as a "citizen's card", in particular by the possible inclusion of a digital signature. As a consequence, discussions started on the extent to which further personal data may be registered on this card on a voluntary basis.

Furthermore the introduction of a personal indicator, in particular in the area of statistics, has been discussed. In particular the question was raised, as to how far abuse possibilities can be technically excluded and data protection guarantees possible when using a personal indicator.

E. Website:

http://www.bka.gv.at/datenschutz/

Belgium

A. Legislative measures adopted under the first pillar

None

B. Changes made under the second and third pillar

A law on cybercrime, adopted on 28 November 2000, has been published in the Official Journal of 3 February 2001.

There has been a long debate between the two chambers of the Parliament regarding the duration of storage of traffic data by telecom operators and service providers, in order to determine whether the duration should be of *minimum* or *maximum* of one year. Finally a duration of a minimum of one year has been decided, against the official opinion of the Belgian Data Protection Authority (Commission de la protection de la vie privée).

The law leaves it up to the Executive to determine the exact duration of preservation. No decree has been adopted yet on that question.

C. Major case law

None

D. Specific issues

Surveillance on the workplace

As a result of the increasing number of questions addressed to the Belgian Data Protection Authority with regard to the monitoring by the employer of the use of E-mail and the internet, the authority has issued an opinion in April 2000 providing guidelines and explaining the legal provisions regulating such surveillance. The opinion refers to the main principles applicable, i.e. general prohibition of interception of telecommunications; transparency and proportionality of the controls; balance of the interests; limited storage of the data. The Data Protection Authority considers that monitoring should be based on limited, objective data, and not on a prior and systematic cognizance of the contents of all data traffic regarding each employee, and it suggests the use of software solutions, by which suspect messages can be specifically targeted.

E-government

The process towards an electronic circulation of information within the administration and between the administration and the public is evolving. In order to facilitate and accelerate the handling of information of individuals – as well as companies – it has been decided to generalise the use of a unique identification number, attributed to each entity. This number will also be the reference integrated in the electronic identity card envisaged for the future. The individual will be requested to use his card in all his contacts with the administration. He will also have the possibility to use it in order to electronically sign documents on-line (e.g. while completing on-line a VAT declaration). While the general objectives and the efficiency aspects of the project cannot be put in question, issues are raised regarding the guarantees taken in order to limit the risks of abuse of the system, considering especially that one of its main goals is to facilitate the circulation of personal information between different administrative services.

E-commerce

The Data Protection Authority has adopted an opinion recalling the privacy principles applicable in the framework of electronic commerce. The opinion describes the circumstances under which personal data are collected on the Internet, and the obligations of the data controller as regards the information of the data subject, and the proportionality of data collected. The Data Protection authority insists in the opinion on the need to obtain the consent (opt in) of the data subject before sending non solicited e-mail messages, and recalls that sending of e-mail using addresses collected on public spaces of the Internet is illegal. The opinion also recalls the main principles applicable to crossborder data flows.

Protection of public data

The Data Protection Authority has received several complaints related to the collection by credit advice companies of data regarding professionals (companies and individuals) involved in litigation with the national social security organisation,

detained in lists for trials at labour jurisdictions. The Data Protection Authority has recalled in an opinion that public data is protected by the privacy legislation, and that their processing is subject to compliance with several principles: the purpose of the collection (i.e. marketing of the data for credit advice) cannot be incompatible with the one originally foreseen (in this case, a publication to give the possibility for third parties to intervene in the trial). The collection of data was considered as incompatible by the Commission, and illegal also because, being judicial data, their processing is forbidden by the law.

Black listing

The personal data of the clients of insurance companies presenting a special risk is processed through a centralised databank. Further to the complaints received by the Data Protection Authority regarding the criteria leading to the communication of the data of some clients to the databank, the Data Protection Authority has raised, in particular, the question of the adequacy of the data transferred, their proportionality, and the information provided to the data subject. The Data Protection Authority has called for a regulatory framework for this kind of activity.

National consumer credit database

The Data Protection Authority has adopted in November 2000 an opinion on a draft legislation destined to enlarge the quality of data integrated in the national consumer credit database, controlled by the national bank. This database will not only include credit information related to defaults of payment, but any information related to a consumer credit contract. The Data Protection Authority has made some observations related to the duration of storage of information related to defaults of payments, and expressed concern about the possible use of the national identification number by the national bank. It has also expressed the wish to be associated to the measures of execution of the new legislation.

E. Website

http://www.privacy.fgov.be

Denmark

A. Legislative measures adopted under the first pillar

Every year several laws and regulations with impact on privacy and data protection are adopted. A very significant measure adopted in 2000 was amendments to the Danish Marketing Practices Act.

The Danish Marketing Practices Act is governed by the National Consumer Agency of Denmark. The most significant amendment to the Marketing Practices Act is section 6 A.

Section 6 A (1) reads as follows: “Where a supplier sells goods, immovable or movable property or work or services to customers, he shall not be allowed to make

calls to anybody using electronic mail, automated calling systems (automatic calling machines) or facsimile machines (fax) for the purposes of such selling unless the particular customer has made a prior request for such calls".

Furthermore according to section 6 A (2) a supplier may not call a specific natural person using other means of distance communication for the purposes of selling goods or services as referred to in subsection (1) above, if that person has asked the supplier not to make such calls, if a list made on a quarterly basis by the Civil Registration System (CPR) includes an indication that the person concerned has objected to receiving calls made for such marketing purposes, or if the supplier has become aware by a search of the Civil Registration System that the person concerned has objected to receiving such calls. Moreover, telephone calls to consumers are subject to the rules on unsolicited calls set out in the Act on Certain Consumer Agreements.

Subsection (2) above shall not apply where the person concerned has made a prior request for the call from the supplier.

Finally the first time a supplier makes a call as described in subsection (2) above to a specific natural person whose name is not included in the CPR list, the supplier shall inform that person in a clear and comprehensible manner of the right to object to calls from suppliers as described in subsection (2) above. At the same time the person concerned shall be given easy access to object to such calls.

B. Changes made under the second and third pillar

None

C. Major case law

All cases concerning the two Registration Acts and the cases concerning the Act on Processing of Personal Data were in the year 2000 decided administratively by the Danish Data Protection Authority.

D. Specific issues

1. An important task of the Danish Data Protection Authority was to give information and guidelines about the new Act on Processing of Personal Data. Furthermore a significant number of notifications and applications were received and handled by the Data Protection Authority as a consequence of the transitional scheme laid down in the act.

2. As to more specific questions the Data Protection Authority expressed its opinion against a suggestion of right of access for police personnel to the central criminal register of offences without personal authorisation codes with a related personal and private password. The suggested arrangement would have made it impossible to detect who had made a search in the register. In accordance with the opinion of the Data Protection Authority the police has based all access to police systems on entry of personal authorisation codes with a related personal and private password.

3. In the year 2000 the Data Protection Authority had some cases concerning genealogy. It was the opinion of the Data Protection Authority that genealogy falls outside the scope of the act, if the genealogist does not disclose data outside the nearest family because the processing of the genealogist is considered processing of data undertaken by a natural person with a view to the exercise of activities of a purely private nature.

If the genealogy is made public for instance on the Internet, the processing can not be considered as an activity of a purely private nature. Therefore the general rules on processing of data have to be applied with. The Data Protection Authority was of the opinion that data about name, year of birth and death as a general rule could be made public without a consent from the data subject.

4. Electronic surveillance of employees has also been an important issue of the Data Protection Authority. The Data Protection Authority has found that an employer has legitimate interests in controlling the use of Internet and email by the employees. The control has to be necessary for the purposes of legitimate interests pursued by the employer and these interests may not be overridden by the interests of the employee. The employee has to be informed in advance in a clear and plain way about the Internet and email control.

On checking emails of the employees the employer is not allowed to read the employee's private emails.

5. In the year 2000 the Data Protection Authority had some cases concerning data made public on home pages. It was the opinion of the Data Protection Authority that data about employees could be made public on a home page without the consent of the employee, if the data were related to the work situation. The Data Protection Authority stated that in general the following data can be made public: name, work area, year of employment, phone number and email address at the place of work.

Data such as a picture of the employee, private address, email address or phone number could only be made public if the employee gives his or hers explicit consent.

6. The Data Protection Authority also had some cases with issues like blacklisting of employees who were dismissed and cases about customers in different business sectors who have accumulated debts or who have defrauded. The Data Protection Authority has given its permission to some of these blacklists on a number of conditions and the blacklist has to have a legitimate purpose.

E. Website

The website of the Data Protection Authority is www.datatilsynet.dk

The website is mainly available in Danish.

Finland

A. Legislative measures adopted under the First Pillar

The Personal Data Act requires that the Data Protection Ombudsman be heard during the preparation of legislative and administrative reforms. The Data Protection Ombudsman issued a total of 43 statements on various legislative proposals to the relevant authorities and Parliament. Together with the Ministry of Justice, the Office of the Data Protection Ombudsman initiated a survey on special legislation, the purpose of which was to promote the achievement of necessary legislative amendments.

Amongst laws relating to the protection of privacy enacted in 2000, one of the most important was the Act on the Status and Rights of Social Welfare Clients (812/2000). Among other things, the Act emphasised the clients' right of self-determination and right of access to information. One of the key aims of the Act on Experiments with Seamless Service Chains in Social Welfare And Health Care Services and with a Social Security Card, designed to promote regional co-operation in the field of public health and enacted on 1 October 2000, was to discover how information technology can be used to promote the protection of privacy.

With the increasing opportunities offered by information technology, pressures to exchange confidential and secret personal data between the authorities increases correspondingly. In such situations, the Data Protection Ombudsman has increasingly had to pay attention not only to the estimation of the relative importance of different interests, but also to the fulfilment of the prerequisites for the technical transfer of information.

The Government submitted on 9 June 2000 a proposal for an Act on the Protection of Privacy in Working Life. The Act was approved by Parliament on 8 June 2001 and the law entered into force on 1 October 2001.

In 2000, preparations were launched for an act on the use of electronic services. The work was based on the E-Directive on Electronic Signatures.

B. Changes made under the Second and Third Pillars

Work for a comprehensive revision of legislation concerning the personal data registers of the police, launched in 1999, continued in 2000. In Finland, the principles of the Data Protection Directive are also applied in the processing of matters coming under the Second and Third Pillars.

C. Major case law

None.

D. Specific issues

As required by the Personal Data Act, the police and public prosecutor heard from the Data Protection Ombudsman in a total of 20 cases. Apart from matters concerning the confidentiality of communication and crimes against confidentiality, the cases mainly involved unlawful use of data in personal data registers, in other words, violations against the provision requiring that data only be used for the purpose they are originally intended for.

One group of cases having special significance with regard to general principles was related to the processing of personal data on data networks and on the Internet. In his statements on making personal data available on the Internet, the Data Protection Ombudsman referred to existing Finnish legislation, under which personal information contained in personal data registers may be made available on the Internet only with the permission of the person in question, or under specific provisions allowing such use.

Under Finnish law, the duties of the Office of the Data Protection Ombudsman focus on preventive work. In addition to the production of general guidelines, information bulletins, models, and model forms for controllers of registers and registered persons, the main focus of activities has been on co-operation with various interest groups. The Data Protection Ombudsman issued an official statement on the following codes of conduct approved in 2000:

- Autoalan keskusliitto ry (The Central Organization for Motor Trade and Repair)
- Suomen Suoramarkkinointiliitto (The Finnish Direct Marketing Association)

Co-operation on the establishment of codes of conduct was carried out especially in the field of public health care and with the Finnish Bankers' Association.
Participation in educational activities was broad (c.150 events) in various sectors.

One issue that produced a particularly heated debate in 2000 was the use of drug tests in schools and workplaces. One of the questions concerned the necessity and accuracy of such information. According to the Data Protection Ombudsman, even if these conditions were satisfied, drug tests may only be carried out, and information on employees gathered, with the informed consent of the person(s) in question. In his statements on the use of drug tests in schools, the Deputy Parliamentary Ombudsman considered it important that conditions for carrying out such testing be regulated by law. Without appropriate legislation, testing should, in the case of school students, only be carried out on the basis of appropriately informed consent. An issue meriting separate consideration is the age at which such consent can be given. In this respect, the age limit of 15 is significant.

During the year, debate increased regarding the position, relative to the Personal Data Act, of electronic press and network publications in general. The use of personal data for publication purposes remains outside the scope of application of the Personal Data Act. Existing Finnish law does not, as such, distinguish between network publications, and newspapers and magazines published in traditional formats. However, since network publishing considerably increases risks related to data security, the Data Protection Ombudsman has taken the position that the legislation on the freedom of expression in the mass media currently under preparation should take

into account the present situation, which has altered considerably in terms of data security. Another question in this context is whether the publication of news, or magazines and newspapers, on electronic networks alters their purpose, depending on various features related to publication and information search.

Another issue that was debated in 2000 was the right of telecommunication operators to use personal data for the provision of localisation services. The matter was discussed in the context of the Act on Data Security in Telecommunications and the Personal Data Act.

One major challenge with respect to the protection of privacy was current activities for the reorganisation of the provision of municipal services and the increasing use of purchased services. Increased networking and the resultant greater use of outsourcing of information processing services in all sectors, as well as the related contractual arrangements, call for a greater focus on systematic planning and on the application of provisions related to the protection of personal data. The Data Protection Ombudsman called attention to the risks for privacy involved in these situations. Such situations also highlight the need for written agreements and sufficiently detailed contractual provisions concerning the processing of personal data. In order to advance matters in this area, the Data Protection Ombudsman co-operated and prepared various models with other authorities and organisations. In the private sector, legislative projects involving the reorganisations of credit institution and insurance activities, for example, brought out several relevant issues regarding the protection of privacy.

The use of electronic identity cards, with the related certification services, has, in principle, been possible in Finland from 1 December 1999. Features enabling the use of electronic services only began to be added to various systems in 2000. In terms of the protection of privacy, the use of such cards has so far been insignificant.

The main focus of activities during the year under review was on the realisation of the registered rights of access to information provided for in the Data Protection Directive. In inspection activities, the focus was on fulfilling the obligation to provide information.

E. Website

http://www.tietosuoja.fi/

France

A. Legislative measures adopted under the first pillar

No new measures.

B. Changes made under the second and third pillar

No changes.

C. Major case law

The French Data Protection Authority (Commission Nationale de l'Informatique et des Libertés , CNIL) referred one case to the courts. It concerns the retention of personal data in its files by the "Ile de France spiritual association of the Church of Scientology" in spite of objections from the person concerned.

There has yet to be a court decision.

D. Specific issues

Application of the principles of data protection in the context of new technologies (Internet, biometry) once again hit the headlines. But more conventional and sensitive areas were also a focus of attention, e.g. epidemiological research - with the introduction of obligatory declarations of HIV seropositivity, and the modernisation of the computer system available to police forces.

In response to complaints, moreover, the CNIL carried out around forty on-the-spot checks, mainly at credit institutions and social housing bodies.

In general terms, it was another year of intensive activity, exceeding the 1999 level with 150 notifications per day concerning files and the processing of personal data, and with 5.900 complaints and requests for advice over the year as a whole. In particular, the number of requests by private individuals for checking files held on them by police forces rose by 21%, leading to 1 300 investigations.

Internet - following an active education effort aimed at new Internet players from 1996 onwards and stepped up markedly in 1998 and 1999 vis-à-vis both the public and private sector, the CNIL carried out a study of 100 e-commerce sites in the spring of 2000 in order to measure the impact of its campaign. The published results show a quite encouraging level of awareness on the part of these sites. In particular, they inform Internet users about possible transfers of data for direct marketing purposes and enable them to state, when inputting their data on line, whether they agree, or not, to their data being put to such use. The two most negative findings to emerge from the study concerned the lack of information on right of access and on the underlying purposes of the cookies used. With a view to improving the situation, the CNIL encouraged professional organisations, portal sites and e-commerce platforms to enhance their performance as relays. What is more, it approached organisations responsible for labelling e-commerce sites. At the end of 2001, the reference systems of the labelling bodies operating in France were in conformity with the provisions of data protection law and with the recommendations of the CNIL.

In late 2000, the increasingly wide-ranging use of the Internet prompted the CNIL to take a further three accompanying steps concerning the new categories of Internet use which had given rise to data protection questions. The first related to the cyber surveillance of employees, the second to health sites and the third to sites intended for children. The work and studies involved, which combined on-site visits and checks as well as concertation with the players concerned, were geared to holding public consultations with a view to drawing up specific recommendations in 2001.

Biometry - the wider use of biometry, especially the use of fingerprints for access control, timekeeping checks and school-restaurant management purposes, came under particular scrutiny. Fingerprints are very specific biometric data, as each of us constantly leave fingerprints (on tables, glasses, school bags, etc) as we go about our daily lives. Thus, a fingerprint database, whatever the reason for its being set up, may become a data comparison tool which can be used for police purposes. Given the sum total of the specific identification features of fingerprints, the setting-up of such a database raises questions concerning individual and public freedoms.

Where essential security considerations called for personal authentification measures, the CNIL approved such applications (e.g. access to premises where national examination papers are stored, to a nuclear waste reprocessing centre and to the Bank of France's security airlock for transporters of funds). On the other hand, the CNIL did not give its approval for the use of such techniques to control access to a school restaurant or for checking compliance with flexitime in a public administration. Finally, the CNIL gave the green light for experimental use for access control and for checking compliance with flexitime based on the recognition not of fingerprints but of hand contours (maintenance personnel at the Louvre museum), which does not involve the same disadvantages.

Two sensitive areas were the subject of major discussions involving the CNIL, the administrations concerned and human rights associations. The first related to epidemiological research concerning seropositivity, the second to the new system for managing crime-related data held by police forces.

In an effort to combat the AIDS epidemic, the law provides for a mandatory declaration which preserves the anonymity of persons who are seropositive. To permit an easier grasp of the associated problems, which concern the reconciliation of epidemiological research designed to obtain a better understanding of HIV seropositivity trends, on the one hand, with the rights and freedoms of those concerned, on the other, the CNIL published a comprehensive report on the subject. When subsequently approached by the French Government concerning measures for the implementation of the legislative text, the CNIL recommended two measures in particular. One was of a technical and organisational nature and was designed to enable data on one and the same person to be compiled over time in such a way as to ensure that the data transferred to the national file remained anonymous. This measure relies in particular on the double encryption of identification data with the aid of irreversible algorithms implemented at source. The second relates to safeguarding the absolute anonymity of persons who go along to anonymous early detection centres offering services free of charge, the aim being not to discourage anyone from being screened: no declaration of seropositivity should be made by the early detection centres operating anonymously and free-of-charge. The Government adopted the CNIL recommendations in their entirety.

The system for the processing of infringements recorded by police authorities (*Système de Traitement des Infractions Constatées* - STIC), made necessary by a law passed in 1995, is a single computer file that pools at national level the data which are collected by Criminal Investigation Departments and feature in the CID reports drawn up at the end of police investigations for submission to the courts. Before giving its

opinion, the CNIL held extensive hearings of professional associations representing police personnel, judges and lawyers, as well as human rights associations.

In response to the numerous issues raised, a number of measures were adopted, primarily concerning the criteria for the inclusion of personal data in the file. In particular, personal data may be included only if they relate to persons concerning whom "there is serious and corroborating evidence that they have participated in the commission of a crime"; on no account may data be input on a mere witness interviewed by the police or on a person who has been wrongly under suspicion or has been the subject of an unsupported denunciation.

Moreover, a technical "locking" mechanism makes it impossible to consult the STIC for administrative purposes in relation to victims. Finally, data relating to victims can be deleted once the perpetrator has been definitively convicted. Where the perpetrator is not identified, storage of data on victims is limited to a maximum of ten years.

The STIC is designed to guide and facilitate enquiries, i.e. to establish links between several cases which have features in common, or to present to a witness or a victim photographs that correspond to the description of the perpetrator. The CNIL stated, however, that this file might be consulted from time to time for preventive purposes, in specific circumstances under conditions of strict security, if the safety of police personnel or other persons were at risk (e.g. summits of Heads of State, large-scale sporting events etc.).

As the setup concerned is not a judicial records system, the CNIL asked that it be forbidden to draw up for inclusion in a dossier relating to criminal proceedings a summary list of the various STIC entries in respect of a particular person.

The length of time for which data may be stored was also the subject of particular attention. The CNIL asked in particular that the time limit for the storage of data relating to certain non-violent and non-serious crimes be reduced to 5 years (instead of 10 or 20 years as initially proposed by the Ministry of the Interior). In particular, the majority of crimes committed by minors, as well as petty thefts, use of narcotics, offences not intentionally committed and road traffic offences fall into this category.

Similarly, it was requested that measures be taken to update the file in accordance with the legal/judicial outcomes of the cases recorded, e.g. acquittals, dismissals or amnesties, which would lead to all data concerned being deleted from the STIC file.

Finally, in addition to certain recommendations relating to security measures, the CNIL also requested that the Director General of the National Police be required to submit to it an annual report on activities relating to the verification, updating and deletion of data recorded in the STIC system.

This approach is embodied in rules adopted by a decree which was passed after the opinion of the CNIL had been sought and which accords with its observations (Decree No 2001-583 of 5 July 2001, OJ of 6 July 2001).

E. Website

France: the CNIL site (www.cnil.fr) was upgraded in 2000 notably by the addition of a Kids' Corner (*espace Junior*) designed to familiarise children with the exercise of their rights.

Germany

A. Legislative measures adopted under the first pillar

Law on framework conditions for electronic signatures and on amending other provisions of 16 May 2001[22]

1. The law on digital signatures has been adapted to comply with the European Union directive on a common framework for electronic signatures. There are three different levels : simple, advanced and authentified signatures. Depending on the level different technical framework conditions apply corresponding to the directive. The law also contains regulations on the recognition of signatures coming from other Member States of the European Union.

2. Law on the adaptation of private law rules of formality and other provisions to modern ways of formation of contracts etc. (agreed on 13 July 2001).

   The update of the telecommunication services data protection law which is included in the law on the adaptation of private law rules of formality - apart from some clarifications and corrections - contains a new section on the right for service providers to process personal data of the respective users in order to improve awareness and start proceedings, when there is indication for misuse of personal data.

   Furthermore infringements to substantial data protection obligations of providers will be classified as administrative offences and will be subject to the threat of administrative fines amounting up to 100.000 DM.

B. Changes made under the second and third pillar

Law on the novellisation of limitations to the secrecy of correspondence, mail and telephone of 26 June 2001 (BGBl. I, S. 1254).

Implementation of the decision of the Federal Constitutional Court of 14 July 1999 on the novellisation of the strategic telecommunication information of the Federal Intelligence Service as well as other modifications to the G10-law (on exemption to confidentiality of communications).

D. Specific issues

A research group of the Bonn university showed that under certain circumstances (manipulation of the signature environment by trojans) procedures for digital signature approved under the old (and probably as well under the new) law on signatures can be infringed upon (the signed document does not correspond to the document indicated to the user).

---

22 BGBl. I, S. 876.

E. Website:

Website of the data protection commissioner : www.datenschutz.bund.de or www.bfd.bund.de
Website of the virtual data protection office: www.datenschutz.de

The websites are regularly updated. The range of issues dealt with the data protection commissioner's website has been extended and includes now :
- data protection and technics
- dataprotection tips for the use of internet and intranet and
- the possibility of encrypted e-mail communication with the Federal Data Protection Commissioner
The range of issues dealt with the site « English texts and documents »includes now :
- the Telecommunications Act,
- the Telecommunications Data Protection Ordinance (TDSV) and
- Forthcoming Legislation in Implementation of Directive 95/46/EC.

Greece

A. Legislative measures adopted under the first pillar

The European Union Directive concerning a common framework for electronic signatures was transposed into Greek law per Presidential Decret.

B. Changes made under the second and third pillar

No major developments to be mentioned

C. Major case law

1. Following to a decision of the Hellenic Data Protection Authority, personal data concerning religion and fingertips of the holder, have been removed from the identity card of Greek citizens. According to the decision, such data was not adequate, relevant and additionally excessive in relation to the purposes for which they were collected and further processed. The above mentioned decision was a very controversial one, especially from the point of view of the Greek Orthodox Church. The decision was appealed in the Greek Supreme Administrative Court, which finally justified the Authority´s decision.

2. According to another decision of the Hellenic Data Protection Authority, video surveillance of public places has to be notified to the Data Protection Authority.

3. The Authority prepared a guideline covering all subjects of data protection in the workplace, especially surveillance of employees' phone calls and e-mails.

D. Specific issues

The revised Greek Constitution includes a new fundamental right to personal data protection (Art. 9A). According to the Constitution, everyone has the right to the protection of his/her personal data. Such data must be collected and processed fairly for specific purposes. Additionally to that, compliance with these rules shall be subject to control by an independent Authority.

E. Website:

http://www.dpa.gr/

Ireland

A. Legislative measures adopted under the first pillar

Legislation to transpose Directive 95/46 into Irish law was not enacted during 2000 but should be done in 2001.

B. Changes made under the second and third pillar

During the year detailed guidelines were published by the Irish Data Protection Authority concerning the credit referencing sector and the whole area of eGovernment.

C. Major case law

As a general comment most data controllers are aware of their responsibilities and act accordingly. However problems did arise during 2000 as now outlined. The Data Protection Authority found that the way in which the Department of Education & Science used the payroll database, to withhold pay from teachers engaged in industrial action, was wrong.

Eircom issued a mailshot to ex-directory subscribers, proposing to disclose some of their details to other telecommunications companies and this was in breach of the Act.

Regarding Irish Credit Bureau the Data Protection Authority has disallowed the practice of disclosing for credit referencing. Under this practice, the ICB, when asked by a bank for the credit history of a named individual, on occasions gave the credit history of a number of different individuals of similar name or address. In disallowing this practice, the Irish Data Protection Authority called on financial institutions to make better efforts to identify customers and establish their proper address.

An individual complained that the Gardaí (the national police force) had not responded properly to an access request. While there were some inaccuracies in the details kept about the individual on the Criminal Records Database (it is vital that this database is completely accurate) the Data Protection Authority did not uphold the complaint that the Gardaí had failed to respond promptly to the access request.

The Data Protection Authority also decided that the printing of customers' addresses on Laser Card receipts was in breach of data protection law. The financial institution involved in this case took prompt steps to correct this matter but it raised questions about security.

D. Enquiries and Complaints

The number of enquiries with the Data Protection Authority rose from 2,200 in 1999 to over 3,100 in 2000 an increase of over 40%. Many of these requests concerned credit ratings, direct marketing, and access requests. Companies contacting the Data Protection Commissioner also queried the new data protection legislation and the process of registration under the Act.

The number of formal complaints in 2000 rose to 131, compared with 105 in 1999 - an increase of 25%. Most complaints involved organisations in the telecommunications and IT sectors, financial institutions, direct marketing companies and public services.

E. Website

http://www.dataprivacy.ie/

Italy

A. Legislative measures adopted under the first pillar

Of the legislative measures taken in the period considered, a few are of interest here although they are related only indirectly to personal data protection. Reference can be made, in particular, to

- a decree regulating establishment, issue, updating and renewal of the permanent electoral card, under which all processing operations concerning personal data must comply with the relevant data protection provisions and be performed under the supervision of the data processor appointed in each local municipality; - a decree including regulations on administrative documents, providing that the documents transmitted to other public administrative agencies should only include data concerning personal status, events and qualifications that are referred to in laws or regulations and are absolutely necessary for achieving the purposes for which they are collected; - a decree concerning the 2001-2003 National Statistics Programme, in whose Preamble the processing of personal data is referred to specifically with particular regard to the information to be provided to data subjects, their right of access to personal data and the specific precautions to be taken in processing sensitive data.

An Act of November 2000 allowed the entities that had not yet managed to adopt the so-called minimum security measures to take advantage – under specific circumstances – of the new, postponed deadline, i.e. 31st December 2000. A prerequisite was the drafting of an official document in which the specific technical

and organisational requirements were to be described that had made it necessary to take advantage of the postponed deadline; the measures included in the plan for upgrading their security systems – whether implemented or yet to be adopted – and the relevant guidelines were also to be specified.

B. Changes made under the second and third pillar

No changes were made in this regard.

C. Major case law

Special importance should be attached to the fact that in 2000 Italy's Court of Cassation was seized for the first time with an appeal concerning data protection matters; this appeal had been lodged against the judgment rendered by an ordinary court – in Milan -, which had reversed the decision taken by the Italian Data Protection Authority Garante on the 19th April 1999.

The issue addressed had to do with the limitations on applicability of the Data Protection Act (DPA) to processing operations performed for journalistic purposes. The facts underlying the case were related to a third party's improper reference to a person's name in the press.

The Court upheld the Garante's decision; indeed it was ruled that the data subject could lawfully request rectification of data allowing her to be identified precisely. Disclosure of the information was considered to be in breach of one among the rights recognised to data subjects by Section 1 in Act no. 675/1996 (the DPA).

As regards the most important category of proceedings instituted before the Garante – i.e., the complaints lodged by data subjects pursuant to Section 29 of the Data Protection Act on account of failure to exercise the rights of access, rectification etc., - the number of the relevant decisions rose in the past year to a total of 187.

Interesting clues can be derived from an analysis of the types of complaint lodged with the Authority, which mostly concern access to employees' personal data and/or personal data included in forensic medical reports, TLC data, processing operations by banks and financial organisations, processing for journalistic purposes.

The decisions rendered by the authority were challenged in eight cases before the competent ordinary courts, as provided for by Section 29(6) of Act no. 675/1996. In three cases where the authority's decision was reversed by the courts, the parties lodged an appeal with the Court of Cassation.

An issue that was raised in this regard had to do with the Garante's capacity to be sued in proceedings instituted before either ordinary courts or the Court of Cassation against the authority's decisions, and with the possibility for the Garante to lawfully be represented in court by the State's General Attorney's Office. The latter was seized with this issue and gave a favourable opinion. It was stressed that appearance in court of the Garante should be more appropriately limited to those cases in which emphasis was put specifically on the public interest to be safeguarded and in connection with

issues of general interest that were related to the proper implementation of data protection legislation.

D. Specific issues

Within the framework of the activities carried out by the Garante, significant instances of the authority's supervisory role are briefly summarised below.

a) Assessment of compliance with data protection principles as regards processing operations for law enforcement purposes. The investigations carried out by the Garante further to reports concerning a few processing operations by the Carabinieri pointed to the lack of harmonised approaches – to be coped with by means of specific legislation – as well as to other problems that can be dealt with in terms of organisational measures. Reference is made here to long-standing practices in respect of which the Garante suggested a number of adjustments in order to, for instance, set out more adequate data retention criteria, diversified consultation policies, regular checks on relevance of the information collected.

In this regard, the Garante carried out a more detailed analysis focussing specifically on the application of data protection principles to these activities in Member States of the European Union– also by way of the workshops that were organised within the framework of the Falcone Project on personal data protection and police and judicial activities, which will be described below.

b) Controls over specific processing operations concerning personal data as performed by the competent intelligence and security agencies. The Garante drew the Government's attention to this issue in order to give increased consideration to the data relevance principle, the selection of available information, the arrangements for accessing and retaining data concerning remote events – although lawfulness and fairness of the relevant processing operations were never disputed.

c) Establishment of large-sized data banks. In connection with the opinion rendered by the Garante to the Ministry for Home Affairs concerning the draft decree setting up a national list of census registers, the authority stressed that data banks should be set up and regulated – especially as regards access by external users – in accordance with specific laws and regulations. This is a prerequisite to ensure transparency of data flows on the basis of homogeneous criteria such as to allow data protection in line with the principles providing that data should be relevant, complete and not excessive.

d) Checking lawfulness of a practice followed by RAI-TV (Italy's Radio and Television Broadcasting Corporation), i.e. to send reminders of the need to pay the yearly subscription charge to potential users of its services. Based on the many reports and complaints received, the Garante investigated the arrangements for sending said reminders to persons who were not included in the lists of subscribers to the broadcasting company's services – with particular regard to the mechanisms of data collection.

e) Assessment and regulation of video surveillance activities. This issue was the focus of considerable activity by the authority on account both of the growing use of this technology and of the sensitivity shown by citizens in this regard. Pending the issue of

ad hoc legislation, the applicable rules can be found in the general data protection Act. Following the many requests submitted by local authorities, which had asked for the authority's opinion in respect of initiatives aimed at implementing electronic surveillance projects, the Garante re-affirmed that the Data Protection Act applies to the processing of images by means of video surveillance systems – irrespective of whether the information is retained or disclosed to third parties.

Based on these premises, the Garante decided to launch a survey by selecting significant locations –such as the downtown areas of a few sample cities including Rome – and assessing the number of (video)cameras deployed. This survey allowed getting a more detailed, precise picture of the video surveillance phenomenon; its findings were presented to members of institutional bodies and journalists. A "decalogue" was subsequently drafted by the Garante and is available on our Web site (www.garanteprivacy.it) for consultation by any person intending to deploy fixed video surveillance systems. Additionally, a few bills were introduced to Parliament in order to regulate use of this technology according to the recommendations made in the said decalogue.

f) Data protection in the workplace. This issue was attached considerable importance by the Garante, which rendered a few decisions concerning, in particular, the distance monitoring of employees – an issue that is closely related to the use of video surveillance techniques -, employees' access to data concerning them – including evaluation data, data on leaves of absence, pay rolls, missions and so on. As to the latter issue, it was pointed out that employers are obliged, in their capacity of data controllers, to provide employees, if they so request, with all the data concerning them. Other important decisions concerned employees' obligation to wear identification badges and the possible dangers for their private lives.

g) Processing of genetic data. The processing of genetic data, regardless of the processor, will have to be authorised specifically by the Garante, as provided for in Section 17(5) of legislative decree no. 135 of 11.05.1999 including the amendments and additions made by Section 16 of legislative decree no. 281 of 30.07.1999.

By way of general authorisation no. 2/2000, the authority specified that the processing of genetic data is allowed with the data subject's consent, in writing, pursuant to Sections 22 and 23 of the DPA and "*with regard to the information and operations that are required to safeguard bodily integrity and health of either the data subject, a third party or the community as a whole*".

The above general authorisation does not apply if the processing of genetic data is necessary to protect the health of either a third party or the community as a whole and the data subject failed to give his consent. In this case, an ad hoc authorisation by the Garante will be required.

Other initiatives by the Garante

In September 2000, the Garante hosted and organised the 22nd International Conference of Privacy and Data Protection Commissioners, which was held for the first time in Italy - in Venice, from the 28th to the 30th of September 2000. The Conference addressed many issues related to privacy and personal data protection; in

particular, the conference motto was "*One World, One Privacy – Towards Electronic Citizenship*".

A significant feature consisted in the participation of supervisory authorities from "new" countries – which shows the step by step expansion of privacy regulations at a worldwide level and points to the shared need for developing harmonised, homogeneous principles in this sector.
Reference should also be made to the agreement reached in the final Declaration – which has come to be known as the "Charter of Venice" and was undersigned by the representatives of the 27 attendant countries. The Declaration is aimed at enhancing the protection of fundamental rights in the light of social evolution and progress as well as scientific and technological development. By re-affirming that privacy is a fundamental human right and a basic component of citizens' freedom, the declaration stressed the general consensus over common principles and criteria applying to data protection as already set forth in OECD Guidelines, Council of Europe Convention no. 108/1981 and European Union directives. Far from being endpoints, the latter instruments are actually a starting point and can give new impetus to the pursuit of their dissemination throughout the world.

Within the framework of the "*Falcone Programme*" – which was sponsored by the European Union in order to enhance cooperation in judicial and customs matters as regards the fight against organised crime - the Garante was granted funds for a finalised project that was focussed on analysing police and judicial activities in respect of the collection, processing and elaboration of data, in the light of the growing cooperative approach adopted in police and, albeit more recently, judicial activities.

Two workshops were organised within the framework of this project; the final meeting, which was held in Rome in December 2000, provided the opportunity for a public presentation of the activities performed.

The discussions held during the workshops and the answers provided in the questionnaires circulated in advance proved quite interesting and helpful; indeed, they showed that - depending on the domestic laws in force - European citizens are actually treated in different ways with regard to a few, important issues. A few instances are provided in this regard by the use of video surveillance techniques, retention period and arrangements applying to telephone traffic data, access by police and judicial authorities to directories of telephone service subscribers, arrangements for collection and processing of genetic data, their use and retention.

The proceedings and the final report concerning the Falcone project were published in English and Italian by the Garante in an ad-hoc booklet.

Another important activity carried out in the past year by the Garante - in its capacity of supervisory authority over the operation of the national Schengen Information System (N.SIS) - had to do with responding to the many requests for verification of the personal data included in the system and lawfulness of the processing operations pursuant to both the Convention Implementing the Schengen Agreement and Act no. 675/1996.

There was a considerable increase in the number of these requests; most of them were submitted directly by data subjects, whilst in a few cases the competent supervisory authorities from other Schengen countries asked for our cooperation in this regard.

In order to enhance expeditiousness of the proceedings and provide timely responses to the many requests submitted by data subjects, the Garante convened a number of meetings with the competent departments at the Ministry for Home Affairs in order to lay down more effective, faster verification mechanisms and procedures.

E. Website:

www.garanteprivacy.it

Luxembourg

A. Legislative measures adopted under the first pillar

No developments to be mentioned.

B. Changes made under the second and third pillar

A law on electronic commerce was adopted on 14 August 2000, and a Grand-Ducal regulation on electronic signatures, electronic payments and the setting up of the Electronic Commerce Committee was adopted on 1 June 2001.
The relevant documents are available at www.chd.lu under *PORTAIL DOCUMENTAIRE, Recherche d'archives, Recherche simplifiée, Mémorial A, commerce électronique*.

A draft law passing the customs convention was presented to the Parliament on 4 May 2001.
The document is available at www.chd.lu under *PORTAIL DOCUMENTAIRE, Recherche d'archives, Recherche avancée. Dossier parlementaire N° 4794.*

C. Major case law

No developments to be mentioned.

D. Specific issues

No developments to be mentioned.

Netherlands

A. Legislative measures adopted under the first pillar

No major developments to be mentioned.

B. Changes made under the second and third pillar

No major developments to be mentioned.

C. Major case- law

An interesting case that deserves to be mentioned is the judgement of the Regional Court of Haarlem of 16 June 2000. This judgement refers to the issue of monitoring of workers at the workplace. In particular, the judge referred in this case to the so-called privatisation of the workplace in our present society. This has as a consequence that an employer should within certain limits accept that private contacts take place during working hours. The employer should guarantee the privacy of these contacts.

D. Specific issues

Video surveillance

In 2000, surveillance by video cameras in public spaces increased substantially. According to the Dutch Data Protection Authority, specific camera use can be a valuable part of a wider package of security measures. The drawback, however, is that ever more refined detection systems are enabling far-reaching supervision of citizens' behaviour. The Data Protection Authority therefore urges a more deliberate policy of restricting application of video surveillance. Also of importance is that the government continues to manage the public domain. The citizen must be seen, but not constantly watched.

Health care

For the improvement of the quality of health care (including accessibility and efficiency), much is expected from the potential offered by information and communication technology. Health care has to handle vast amounts of data, for direct patient care and financing, as well as for research and policymaking. The Data Protection Authority points out that within this framework too little attention is being paid to the protection of personal data and professional medical secrecy. This applies especially to the conditions that pertain to the increasing role of health insurers. The Data Protection Authority also points out the consequences of this for the revision of the system of health care.

The recent plans in the sector for care assignment and waiting list management under the Exceptional Medical Expenses Act envisage an extensive collection of data on each patient. The Ministry of Health, Welfare and Sports, Dutch health insurers and the Health Insurance Board are seeking a national system of registration based on the Exceptional Medical Expenses Act, whereby the data can be identified at the level of the individual. The Data Protection Authority has informed parties involved about its strong doubts with regard to the legitimacy of this approach.

Privacy and Internet

In response to public anxiety and questioning, the Data Protection Authority studied various aspects of the private use of Internet and e-mail. Many Internet Service Providers collect

clients' data and behaviour on the Internet for commercial purposes. The Authority has come to the conclusion that the protection of personal data by Internet Service Providers is failing badly. A report was produced following research on controls applied by employers on the use of Internet and e-mail at work. Guidelines were drawn up for a realistic approach to this control on the basis of specific consideration of the interests of the employer and the employee. In order to fight crime through the Internet, law enforcement institutions are pursuing extensive powers of investigation. The Data Protection Authority has urged the Lower House to respect the limits of the constitutional state in the projected Convention on Cybercrime (Council of Europe).

E. Website

www.cbpweb.nl

Main Publications in 2000

Klant in het web (Client on the Web), June 2000; addressing privacy protection on the Internet.
Herkomst van de klant (Origin of the Client), October 2000; an investigation of the tensions associated with the inclusion or exclusion of people on the basis of race or ethnicity in the marketing of products.
De gewaardeerde klant (The Valued Client), October 2000; on the evaluation of creditworthiness whereby third parties such as credit rating agencies, are involved.

Politiegegevens beschermd (Protecting police data), June 2000; an explanation of the closed regime for data provision in the Police Files Act.

Goed werken in netwerken (Working well in Networks), December 2000; a report on the control of e-mail and Internet use at work.

Zorg voor gegevens bij indicatiestelling – aanbevelingen voor de praktijk van indicatiestelling (Care for data on medical diagnosis – recommendations for practice in diagnosis information), August 2000; report on the possibilities and limits in collecting, using, transferring and recording patient's data to determine the diagnosis for care provision within the scope of the Exceptional Medical Expenses Act.

Bankverzekeraars en privacy (Bank insurers and privacy), November 2000; report on the actual processing of personal data within financial conglomerates.

Privacy-Enhancing Technologies: the path to anonymity was reprinted due to unremitting demand.

Portugal

A. Legislative measures adopted under the first pillar

No developments to be mentioned.

B. Changes made under the second and third pillar

No developments to be mentioned.

D. Specific issues

The Portuguese Data Protection Authority legalised about 500 databases, 80 of those in the telecommunications sector. 150 complaints were filed (30 in the telecommunications sector). The Portuguese Data Protection Authority carried out 135 inspections *in loco*, most of them resulting from citizens' complaints, but also from verification procedures on their own initiative, including an audit to a telecommunication operator using GSM.

Concerning sanctions, the Data Protection Authority applied 3 fines (for lack of notification, for lack of the right of information and for undue video surveillance), and blocked the site of the Ministry of Justice, which had on-line in full text the criminal decisions of the Supreme Court, identifying minors, victims of crimes such as rape, etc. All decisions were made anonymous in 30 days.

There have been some preparatory works regarding a Code of Conduct for the pharmaceutical industry.

Data concerning "bad payers": the Data Protection Authority appreciated a request from a consumer credit company, which intended to process personal data on clients with debts to mobile phone operators. This "blacklist" was to be acceded by all operators. The Data Protection Authority did not authorise that data processing, once it would not be possible with the current legal and contractual dispositions.

Opinion on the Cyber crime Draft Convention: the conclusions of the Portuguese Data Protection Authority are similar to the opinion given by the Article 29 Data Protection Working Party.

Confidentiality: the Portuguese Data Protection Authority evaluated the levels of data confidentiality, considering that communications' contents and traffic data are protected by the telecommunications seal, as well as the billing data and debts data are protected by professional secrecy. Therefore, the service provider can refuse, even to a court, to give those data. In case of a criminal suit, the service provider can also refuse and if the judge considers the requested information of utmost importance, he has to appeal the question to a superior court, which decides if the service provider must disclose the data. In relation to the identification of the subscriber, his address and telephone number – unless the subscriber has requested confidentiality – these are not protected data, from the telecommunications perspective.

E. Website

http://www.cnpd.pt/bin/principal.htm

Spain

A and B - Changes made under the first, second and third pillar

- Pursuant to **Royal Decree No. 994/1999 of 11 June 1999** approving the regulation on the security measures for automatic filing systems containing personal data, the basic-level security measures for all automated files and the medium-level security measures for certain kinds of files came into force.

- **Data Protection Authority Instruction No. 1/2000 of 1 December relating to the rules governing international data movements** was published in the *Boletín Oficial del Estado* of 16 December 2000. It sets out the guiding criteria which the Data Protection Authority considers in relation to the processing involved in international data transfers. This clarifies the Data Protection Authority's procedure in enforcing the rules on international data movements, and is hugely useful in that it incorporates the various provisions regulating this matter into a single text. The Instruction is in two sections, the first of which refers to the criteria applicable to any international data transfer while the second refers to specific transfer cases.

- **The Data Protection Authority Ruling of 30 May 2000 approving the standard notices on paper, magnetic and telematic media for applications to have public and private files entered on the General Data Protection Register** was published in the *Boletín Oficial del Estado* of 27 June 2000. With the entry into force of the new Law No. 15/1999 on the protection of personal data, it was necessary to issue new instructions and to publish new forms for registration, including clearance for giving notice of processing via the Internet.

C.- Major Case Law.

3.1 Jurisprudence of the Constitutional Court

The Constitutional Court issued **three** judgements with a bearing on the activity of the Data Protection Agency in 2000.

These included Judgements No. 290/2000 and No. 292/2000 of 30 November 2000 following challenges to the constitutional validity of the current Law No. 15/1999 on the protection of personal data and its precursor, which it repealed, Organic Law No. 5/1992 on Data Protection.

1.- Judgement No. 290/2000 resolved the various challenges to the constitutional validity of Organic Law No. 5/1992 lodged by the Executive Council of the Generalitat de Catalunya, the Parliament of Catalonia, the Ombudsman and 56 Members of the Parliament.

Essentially. this judgement focussed on whether certain Articles of the previous Data Protection Law were in breach of the distribution of powers between the State and the Autonomous Communities laid down in the Spanish Constitution in respect of the duties and powers attributed to the Data Protection Agency in the Data Protection

Law. The Court concluded that the provisions were entirely consistent with the distribution of powers enshrined in the Constitution.

2.- Judgement No. 292/2000 upheld the challenge to the constitutional validity lodged by the Ombudsman against Articles 21.1 and 24.1 and 2 of the current Organic Law No. 15/1999 on the protection of personal data. This judgement is of vital importance for data protection in that it emphatically recognises the fundamental right to the protection of personal data as an autonomous right stating that "the subject protected by the fundamental right to data protection is not solely limited to an individual's private and personal data, but to any kind of personal data, whether strictly private or not, knowledge or use of which by a third party may affect his or her rights, fundamental or otherwise, because it does not solely concern individual privacy, which is protected by Article 18.1 of the Spanish Constitution, but personal data".

The judgement found that certain indents of Articles 21 and 24 of Organic Law No. 15/1999 on Data Protection referring to different cases in which data could legitimately be transferred or communicated between public administrations were in breach of the Constitution and void, and restricted the exceptions to the rights of information and access in relation to processing undertaken in the public sector.

3.- The third significant judgement was **No. 202/1999** concerning employers' processing data on workers' health. The Constitutional Court upheld an appellant's right to privacy pursuant to Articles 18.1 and 4 of the Spanish Constitution. The Court found that the applicant's right to privacy was breached when, without express consent and without any contractual link to this effect, the employer included information on the medical diagnosis of an employee in a database on sick leave records which was maintained not for the purpose of preserving workers' health but for monitoring absenteeism. It also found in favour of the applicant in recognising his right to delete such data.

It took the view that the processing undertaken by the enterprise was disproportionate for the reasons stated.

3.2 Judgements delivered by the administrative courts

Fifty-four administrative appeals were lodged against Data Protection Authority rulings in 2000, in most of which the courts found in the Data Protection Authority's favour. This represents an increase of 86% on the judgements delivered in the previous year.

The issues at stake were mostly the following: solvency and credit ratings; banking and insurance; commercial canvassing and advertising activities; the transfer of data from the Population Register or the transfer of data between entities in the same group.

By way of example, some particularly relevant judgements may be summarised as follows:

- Judgements delivered over the past year have reiterated others handed down in 1999, to the effect that the data contained on the electoral register should not be incorporated into any source which is accessible to the public, for which reason it is illegal to collect them for the purposes of advertising and canvassing.

- One judgement on the transfer of data from the Population Register confirmed the penalty imposed by the Data Protection Authority on a Municipal Council for transferring the data contained on the Municipal Register of Population to a private body, as a result of which a case was subsequently taken to the Court of First Instance.

- The courts also backed the Data Protection Authority's view that the transmission of data between enterprises in the same group constitutes the transfer of data, and therefore requires the consent of the party concerned or legal powers to take this course.

- Another significant judgement rejected an appeal against a penalty ruling by the Data Protection Authority. In this case, an individual complained that he had received an advertising catalogue from an entity which had had his data transferred from another which was an accredited processor for a third party to which the data subject had provided his data when purchasing a specific product. The judgement found that there was a transfer of data not covered in the contractual relationship for the provision of services, in that a processor is not entitled to cede data to third parties under any circumstances – even for the purposes of conserving them - nor is he entitled to use them for any purposes other than those laid down in the service contract.

D. Specific issues.

There has been a remarkable increase in citizens' interest in better information on the scope of the right to data protection. This was reflected in some 19.262 enquiries to the Data Protection Authority in relation to its **Duty to Inform Citizens.** Most of these – 14.420 (25% more than the previous year) were handled by telephone; 2.964 (70% more than the previous year) in writing, and 1.878 (63% more than the previous year) were dealt with in person. The 1.173.056 hits recorded on the Data Protection Authority's web site represented an increase of 132% on the previous year. The site has a frequently asked questions section covering the commonest concerns: advertising deliveries; telephone billing data; telephone directory data; the scope of the Law; access to a known processor; access to the Data Protection Authority on personal data; credit and solvency files - solvency records including data from sources which are accessible to the public; the addresses of solvency information files; the registration of files; instructions for declaring data files; security documents and security measures in general. Enquiries were also received concerning industrial relations; health data; insurance; telecommunications; Internet and web pages; exercising the rights of access, correction, cancellation and objection and data transfers.

Enquiries by data controllers over the past year increased by 63.78% on those which the **Legal Unit** dealt with the previous year. Of the total, 235 were enquiries by public administrations – as data controllers in public ownership - and 371 were enquiries by data controllers in private ownership.

The Data Protection Authority was asked to clear 21 provisions, of which the following deserve special mention:

- the draft Royal Decree setting up and governing the Interministerial Commission on combating activities in breach of the rights of intellectual and industrial property;
- the second draft Ministerial Order setting up the Committee in the Ministry of Health and Consumer Affairs for managing a census of people with haemophilia and other congenital coagulopathies who have developed the hepatitis C virus as a result of treatment received in the public health system, and the regulation on creating the files relating to this;
- the draft Royal Decree on the entering of Spanish citizens on the Registers of Consular Offices abroad;
- the draft Royal Decree implementing the internal control regime maintained by the Social Security Inspectorate-General;
- the proposal for a regulation with the status of a law for updating the regulation of the *Banco de España*'s risk assessment centre (CIRBE);
- the draft Ministerial Order regulating the Ministry of the Interior's automatic files of personal data on DNA;
- the draft preliminary Data Protection Law of the Community of Madrid;
- the proposal for a law from the Socialist Group relating to the measures necessary to prevent the mass processing of personal data by telephone operators;
- the draft Royal Decree approving the Regulation on Health Protection against Ionising Radiation;

There was also a great increase in applications to have files entered on the **General Data Protection Register**. A total of 10.512 requests to register files required 25.760 registration operations, given that each request contains more than one notification for registration purposes. This represented a 400% increase on the previous year. It has been possible to apply to register files via the Internet since July, and the applications received by December gave rise to 2.445 operations to register, amend or delete private files and 21 for public files, outstripping the operations completed by sending in magnetic media in the case of private files – 1.995 over the whole year.

As of 31 December 2000, a total of 249.209 files had been placed on the General Data Protection Register, of which 31.155 were in public ownership and 218.054 in private ownership. Of the public files relating to activities under the third pillar registered in 2000, six concerned the operations of the Security Forces for police purposes - out of a total 2.063 registered up to 31 December - and 13 concerned judicial proceedings - out of a total 880 registered by 31 December 2000.

It should also be mentioned that 1.352 international data transfers were declared to the Data Protection Authority, 51 of which are in public ownership and 1.301 in private ownership.

Of the files declared in 2000, 272 entailed international data transfers.

It should also be emphasised that there was an increase in complaints filed by citizens and, therefore, in the **data inspection** activities pursued by the Agency. There was a considerable year-on-year increase in these procedures, targeting controllers of data in both private and public ownership. In 2000, the Director of the Data Protection Authority issued 622 final rulings in administrative cases following complaints, procedures and appeals.

The inspection activities could be divided into **two large groups**: those arising from **complaints** lodged by individuals citing a breach of the principles laid down in the law in force, and work under **Sectoral Inspection Plans** to check the level of compliance with the rules on the protection of personal data in both the public and the private sectors.

Work in response to **complaints** concerning **files in private ownership** concerned in particular the processing of personal data by **telecommunications services:** data processing without consent, the principle of data quality implying the obligation that these be accurate and updated to provide a true picture of data subjects; compliance with the data protection regulations specific to the telecommunications sector, Law No. 11/1998, the General Law on Telecommunications and Royal Decree No. 1736/1998 approving the regulation implementing Title III of the General Law on Telecommunications concerning the universal telecommunications service (both of these transpose Directive 97/66 concerning the processing of personal data and the protection of privacy in the telecommunications sector into the Spanish legal system); the processing of personal data on the **Internet**: undue disclosure of personal data; the forwarding of messages by electronic mail or the use of data collected on the Internet for purposes other than those for which they were originally collected; the case of the Association Against Torture, initiated following a complaint and in which the Director of the Data Protection Authority imposed penalties because the data subjects had not given their consent; for illegal transfer of data and as this file entailed criminal offences beyond the scope provided by law. **Direct marketing and advertising** was also one of the commercial activities which gave rise to the greatest number of complaints: direct mailing; data transfers; processing without consent or non-deletion. The **provision of solvency and credit rating services** also provoked a significant number of complaints and therefore created considerable work for the Authority. The **health** sector was also concerned – the most striking complaints involved illegal transfers of personal health data. Other complaints received, albeit in lesser numbers than in the sectors mentioned above, concerned **professional colleagues**, **political parties** and **trade unions.**

Where privately-owned files in this same area were concerned, an inspection of the television programme “Big Brother”, conducted **on the initiative of the Director of the Authority**, led to penalties being imposed for breach of the legal precepts that express consent is required for processing especially protected data, that data subjects' information rights should be upheld, that the corresponding security measures should be taken and that guarantees required by law in relation to data transfers should be in place.

One important case began with reports from various communication media that the personal data of a major telephone operator's subscribed clients could be accessed via the Internet. The preliminary investigations established a series of facts as a result of which sanctions were applied for failing to meet the data controller's duty to maintain security and for breaching the Security regulation which implements this precept.

Another noteworthy case arose in summer of 2000, when the Data Protection Authority received computer media containing over twelve thousand user codes and passwords allegedly corresponding to Internet users who had contracted services with the owner of the portal concerned. Inspections were launched to determine whether the law had been breached in relation to the loss of confidentiality on those data. The procedure concluded when sanctions were imposed for failing to meet the obligation to take the technical and organisational measures necessary to guarantee data security and for failing to delete the data once the purpose for which they were collected had been achieved.

It should be stressed that **Proactive Sectoral Plans** are intended to establish how personal data are processed in the sectors inspected with a view to disciplinary action in the light of the Organic Data Protection Law. On concluding these inspections, pursuant to the powers conferred on him by the Authority's statute, the Director of the Data Protection Authority usually issues recommendations which it is incumbent on the entities inspected and every business in the sector to note and comply with by adapting their processes to the principles and requirements of the Organic Data Protection Law.

In 2000, a series of **Recommendations** were issued further to the Proactive Sectoral Plans carried out in 1999, which concerned the State Tax Administration Agency, the Directorate-General of Traffic, **the health sector (**the Gómez Ulla General Military Hospital, the Alicante Penitentiary Psychiatric Hospital, the National Epidemiology Centre -the National AIDS Register) and the **private research** sector.

The Data Protection Authority attached particular importance to the Proactive Sectoral Plans in 2000, and **proactive inspections** were carried out concerning **e-commerce**; **Internet service providers**; **card management in hypermarkets**; the **telecommunications sector** and the ***Consorcio de Compensación de Seguros*** (Insurance Clearing Consortium).

Particular mention should be made of the inspections of data protection carried out in the **e-commerce** sector. These took account of private self-regulation initiatives in this area: that of the Spanish e-commerce and Direct Marketing Association in its Code of Ethics on Personal Data Protection on the Internet - which was entered on the General Data Protection Register in 1998 - and the Code of Professional Standards of Internet Service Providers of the Multi-sectoral Association of Spanish Electronic Enterprises.

The conclusions drawn from that Proactive Sectoral Plan indicate that web users are not always (27 %) informed of the name of the data controllers for files on which the personal data collected are stored. Similarly not all data controllers (36%) for the web pages analysed have declared their files to the General Data Protection Register, bearing in mind that it is obvious in virtually every case that data are collected from the web pages concerned. A further important point is the fact that, in most cases,

users are obliged to register before placing orders, whereupon they have to provide their identifying data. In security terms, it was established that only 54% of the web pages examined used HTTPS protocols to set up a secure channel between servers and users for communicating personal data.

The Data Protection Authority's most significant data inspection measures concerning **files in public ownership** focused on the following central government bodies: the State Tax Administration Agency - which had also featured in complaints received from taxpayers-; the General Treasury of Social Security; the National Social Security Institute, as a result of which the Director issued Recommendations obliging the Institute to uphold the right to information when collecting data and to secure data subjects' express consent for processing data such as those concerning health derived from disabilities and other especially protected data such as child support payments and alimonies paid to spouses; the National Employment Institute - which had been the subject of complaints received- ; the Directorate-General of Traffic; the Delegation of the Government in Castilla y León; the Ministry of Defence; the Ministry of Education and Culture and the Ministry of Foreign Affairs.

Inspections in response to **complaints from individuals** were also carried out in the offices of the Autonomous Communities of the Balearics; La Rioja; Asturias; Andalucía and Valencia. Proactive inspections were carried out in the offices of the autonomous Communities of Murcia and Catalonia and in local government offices.

Six inspections were launched in the State Security Forces.

Seven rulings were also issued in response to a number of **requests for cooperation** under Article 114.2 of the Schengen Convention **from the President of the *Commission Nationale de L'Informatique et des Libertés* (CNIL)**, the competent authority for data protection in France. These sought access to, and cancellation of, files on the **Schengen Information System** concerning individuals to be denied entry to Schengen territory, whose data had been entered by Spanish Authorities. Action was therefore taken to establish whether those individuals' data had been correctly registered under current legislation. In every case, the files and records of the General Commission on Foreign nationals and the documents of the Directorate-General of Police were examined, and it was established that those individuals had been expelled from national territory pursuant to judicial or administrative rulings and banned from entering the country. In every case investigated, the CNIL was informed of the action taken and of the grounds for entering these individuals on the SIS.

One case of cooperation between the CNIL and the Data Protection Authority deserves mention: In November 2000, the Authority received a declaration from the CNIL that a Spanish entity which compiled and printed a Europe-wide guide to professional services had billed some French residents - one of whom had lodged the complaint - for requests to have their data inserted in one of the entity's yearbooks even though no such requests had been made. The Director ordered the Data Inspectorate to take all due steps to clarify matters. On completing the inspection, it was decided to keep the steps taken on record because it was established that the mailing/dispatch had used data on professionals obtained from sources accessible to the public - and specifically telephone directories from several European countries

including France - and that the subsequent data processing had been undertaken with the express written consent of the data subjects.

On two occasions in 2000, the Director of the Data Protection Authority appeared before the Constitutional Committee of the Congress of Deputies to discuss the Data Protection Authority's Annual Report for the purposes of parliamentary supervision of the Data Protection Authority's activities and to discuss the key subjects relating to the Data Protection Authority's activity raised by the Parliamentary groups. These included, for example, data protection in international transfers, within public administrations or questions relating to the Security Measures Regulation.

On 12 June 2000, the Director of the Data Protection Authority signed on behalf of the Authority a **Protocol on information cooperation between the Data Protection Authority and the Higher Council of Official Chambers of Commerce, Industry and Navigation** for the purposes of directing, coordinating and establishing common criteria for all the Chambers with a view to determining and demarcating the rating of their files and cooperation between the parties on resolving interpretative questions on the application of Organic Law No. 15/1999 and setting up working groups to establish the appropriate coordination procedures.

On 13 April 2000, the Director also signed on behalf of the Data Protection Authority a **Protocol on Cooperation with the General Council of Notaries Public** which envisages setting up working groups to make it possible jointly to provide clarification, information and cooperation on measures permitting the law best to be upheld in individual cases.

The Protocol on Cooperation signed with the Professional Union combining Professional Colleges and the General Councils of the various professions on 15 June last year should also be mentioned.

All these initiatives aimed to seek out and identify the main problems facing groups of data controllers and to provide a uniform response on applying the Data Protection Law for the representative organisations to disseminate among their members.

E. Website:

https://www.agenciaprotecciondatos.org/

Sweden

A. Legislative measures adopted under the first pillar (excluding Directives 95/46/EC and 97/66/EC)

Specific register statutes for example:

Act (2000:224) on Land Register (Lagen om fastighetsregister) regulates processing of personal data in the Land Register and states that the National Land Survey shall keep a Land Register for the purpose of providing information about real property.

Act (2000:832) on qualified electronic signatures
The purpose of the Act (2000:832) on qualified electronic signatures is to facilitate the use of electronic signatures and the Act implements the EC Directive 99/93 on electronic signatures. Section 16 regulates collection of personal data and states i.a. that a body that issues certificates must only collect personal data from the person that the data relates to or with his/her explicit consent.

Act (2000:344) on the Schengen Information System
The Act (2000:344) on the Schengen Information System states that the National Police Board shall keep a register for the purpose of being the Swedish national section of the Schengen Information System (SIS). The Act regulates the National Police Board's processing of personal data within the Swedish section of the SIS.

B. Changes made under the second and third pillar

Specific register statutes for example:

Act (2000:344) on the Schengen Information System

C. Major case law

The City Court of Gothenburg fined a nurse for unauthorized access to data. When a minister of the Swedish Government fell ill and was taken to hospital, where he subsequently died, it was noted that a great number of people from the hospital staff had accessed his medical record. An investigation showed that several of these persons had not been involved in the actual treatment of the minister and consequently should not have had access to the data. The decision has been appealed against.

An employee in a church parish presented information about her colleagues on a website without having obtained their consent. A few of her colleagues resented the presentations and the employee reported herself to the police for investigation of whether she was guilty of offence against the Personal Data Act. Legal proceedings were taken and the Data Inspection Board was asked to give an opinion. The Board noted that the published personal data should not have been processed without consent and that some of the data were sensitive (data about health). The Board also noted that personal data had been transferred to third countries in contravention of the Personal Data Act and that the processing had not been notified according to the Act. However, the Board also observed that according to a recent amendment of the Act, a sentence shall not be imposed in petty crimes. The District Court, however, did not find that the crime was petty and ordered the woman to pay fines for breach of the Personal Data Act. The Court’s decision has been appealed against and the court of appeal has demanded an opinion from the EC Court of Justice.

D. Specific issues

The Data Inspection Board published an information leaflet on Personal data and the Internet. The Board also handled cases concerning the issue of publishing personal data on the Internet and exemptions for processing operations which are carried out for journalistic purposes.

Following a discussion in media about the handling of credit information and especially inaccurate data in such information, the Data Inspection Board carried out supervision on credit information activity in a joint project with the Swedish Financial Supervisory Authority. The supervision resulted in a report, "Missvisande kreditupplysningar – åtgärder och förslag", which has been published on the Data Inspection Board website.

The Swedish Government set up a commission of enquiry to investigate privacy in the work place. An employee of the Data Inspection Board is appointed as expert in the commission of enquiry.

E. Website

www.datainspektionen.se

The United Kingdom

A. Legislative measures adopted under the first pillar

The United Kingdom introduced legislation to enable individuals to have greater access to information held by public bodies.

The Freedom of Information Act 2000 allows individuals access to all types of information held whether personal or non personal. It also requires public authorities to adopt and maintain publication schemes setting out their arrangements for publishing information. This legislation, which will come fully into force by 30th November 2005, is to be enforced by the Information Commissioner.

A further piece of legislation that impacts both on the Data Protection Act and more widely is the Human Rights Act 1998. This came into force in October 2000 and for the first time incorporates the European Convention on Human Rights into United Kingdom law. This Act contributes significantly to the legal framework within which the Information Commissioner interprets and applies the Data Protection Act. It affects how she, as a public body, deals with those who approach her and those that she regulates.

The Regulation of Investigatory Powers Act 2000 introduced provisions, regulating interception of telecommunications systems, covering for the first time private systems such as those in most workplaces. The Act implemented Article 5 of Directive 97/66/EC. It also introduced controversial provisions giving powers to law enforcement agencies for the investigation of electronic data protected by encryption. On its own the RIP Act would have outlawed the interception by employers of electronic communications in the workplace. The Lawful Business Practice Regulations 2000 were therefore introduced in order to make lawful the interception of communications by employers in particular circumstances. These Regulations did not remove the obligations on employers to comply with the Data Protection Act but the way in which they were introduced led to considerable misunderstanding. The Information Commissioner has sought to clarify that the Regulations do not give

employers a right to routinely monitor the communications of their workers regardless of data protection requirements.

B. Changes made under the second and third pillar

In 2000 as a result of the Europol Convention a data protection Joint Supervisory Body was established which adopted a systematic approach to the auditing of Europol. The Information Commissioners office took an active part in this work. In another area, that of the Schengen Agreement, the United Kingdom has now agreed to join the Schengen arrangements for sharing police data, and further, will attend the Schengen Data Protection Common Control Authority as an observer.

C. Major case law

In 2000 formal enforcement action was taken against two companies for contraventions of the Telecommunications (Data Protection & Privacy) Regulations 1999 in respect of the sending of unsolicited direct marketing faxes. The enforcement action was based upon numerous complaints received by the Commissioner. The companies appealed against the action.

Prior to a hearing and after extensive regulations both companies agreed to submit to raised enforcement notice. The Commissioner continues to monitor the compliance of these organisations along with others in order to ensure compliance with the Telecommunications Regulations. In doing so she also served three other organisations with Preliminary Enforcement Notices in 2000.

D. Specific issues

The Data Protection Act 1998 requires the Commissioner to promote the following of good practice and the observance of the requirements of the Act by data controllers. In order to do so she can prepare and disseminate codes of good practice for data controllers. The first such code, on the subject of closed circuit television monitoring was issued in July 2000. This code was well received by data controllers and individuals. It was intended to give clear and unambiguous advice as to how to comply with the law and what would be considered to be good practice in the use of CCTV systems in public places.

The Commissioner also instructed her staff to work on producing a similar code of practice on the use of personal data in the employer/employee relationship. A draft was issued in October 2000 and it attracted considerable interest particularly in relation to monitoring e-mail and Internet access in the workplace. Work on this project is still ongoing. The scope of the final code will cover not just the traditional employer/employee relationship but also the wider context to including such groups as volunteers, agency and contract workers.

In August 2000 the Commissioner’s office also commenced a joint initiative with the Department of Social Security and the Inland Revenue. This initiative, the Baird Project, was designed to clamp down on people and organisations that unlawfully and systematically seek to obtain personal data for third parties. This initiative has been successful and is likely to result in a number of prosecutions.

In the UK the electoral register, containing the names ad addresses of everyone entitled to vote, has always been available for sale to the public. It has been used for marketing, debt tracing and a range of other purposes. Following pressure from the Information Commissioner and others the Representation of the People Act 2000 provides for two electoral registers to be produced. The first for electoral purposes is the full register, on which all those eligible are to have their details recorded. The second is an edited version. Voters would have the option to choose whether to have their details included on this register or not. Only the edited register will be available for sale. Regulations to bring the new arrangements into effect are awaited. A crucial question that remains is who will have access to the full register and for what purposes.

In 2000 the Commissioner ran a large media campaign to inform individuals of their rights under the Act and also to promote awareness of data protection. This campaign included television advertisement on one of the major television channels in the United Kingdom. Local rate telephone numbers were linked to a mailing house that dispatched literature outlining individuals' rights to those who requested information. A survey revealed that there was a 19% awareness of the advertising campaign amongst respondents.

The introduction of the Data Protection Act 1998 and the media campaign have contributed in part to an increase in the Commissioner's workload. There are now over 220,000 entries on the register of data controllers despite significant exemptions from the requirement to notify introduced by the new Act. The enquiry line handles around 55,000 calls per year. Complaints from data subjects, which have become request for assessments under the new law number 8,000.

In 2000 the Commissioner actively encouraged secondments into and out of her office. These included the part time secondment of an Assistant Commissioner to the Performance and Innovations Unit at the Governments Cabinet Office to work on a yet to be published report on privacy and data sharing.

E. Website

http://www.dataprotection.gov.uk/

1.5. European Union and Community activities

1.5.1. Data protection in Community Institutions and bodies

The Treaty of Amsterdam introduced a new Article 286 in the Treaty establishing the European Community. This provision lays down that, from 1 January 1999, the Community institutions and bodies must apply the Community rules on the protection of personal data, as set out essentially in Directives 95/46/EC and 97/66/EC. It also lays down that the application of those rules must be monitored by an independent supervisory body. Moreover, the same concern was behind the inclusion of the right to the protection of personal data in Article 8 of the Charter of Fundamental Rights of the European Union.

According to this mandate, the Commission had submitted on 14 July 1999 its proposal for a Regulation on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community. The Commission, the Council and the Parliament expressed then their common aim to get the Regulation approved in the first reading of the co-decision procedure. Accordingly, and following a political compromise on a consolidated text, the European Parliament voted on a number of amendments on 14 November 2000; the Commission accepted these amendments and put forward its modified proposal; and the Council unanimously approved it on 30 November 2000. The Regulation was thus adopted on 18 December 2000.

The Regulation lays down a series of principles to which the processing of personal data by the Community institutions and bodies is subject. Alongside these substantive provisions, the Regulation sets up an independent supervisory authority, the *European Data Protection Supervisor*, which is entrusted with ensuring the application of the provisions of the Regulation.

1.5.2. Draft directive on the protection of privacy and personal data in electronic communications

The Commission proposed the draft privacy directive[23] as part of the telecommunications review package which comprises several proposals with a view to updating the regulatory framework to a converging technological environment. The draft privacy directive is intended to replace Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector, which was adopted by the European Parliament and the Council on 15 December 1997 and had to be transposed by 24 October 1998 at the latest.

The proposal is not intended to create major changes to the substance of the existing Directive, but merely adapts and updates the existing provisions to new and foreseeable developments in electronic communications services and technologies.

The majority of provisions of the existing Directive are therefore carried over in the new proposal, subject to minor drafting changes.

One of the regulatory principles as set out in the context of the 1999 Review of the regulatory framework for electronic communications services, is the aim to create rules which are technology neutral, this is not to impose, nor discriminate in favour of, the use of a particular type of technology, but to ensure that the same service is regulated in an equivalent manner, irrespective of the means by which it is delivered.

The proposed changes concern definitions and terminology (for example in order to confirm that the directive applies to the provision of e-mail services), traffic data (clarify that also Internet traffic data are covered), location data (allow the use of

---

[23] Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (COM(2000)385, 12 July 2000, OJ C 365 E/223 of 19.12.2000.

location data for the provision of added value services with consent of the user), directories (give users full choice as to whether and how they want to be listed in phone, handy, e-mail directories), unsolicited communications (harmonisation of national rules by requiring prior consent of addresses of marketing messages via e-mail) and the privacy compliance of software and hardware used for electronic communications services.

The opinions on this draft directive issued by the Article 29 Data Protection Working Party[24] have been taken into account.

1.5.3 Privacy Enhancing Technologies

Beside the technical projects launched by the IST Programme in the area of privacy enhancing technologies, we worked on the eEurope action on "promoting privacy-enhancing technologies and supporting their deployment, including proper codes and the consolidation of practices". The action builds on and leverages the work carried out for us by the JRC as part of the institutional role. Two are the main activities planned for this action.

The former focuses on organising thematic workshops with all stakeholders:

- A workshop on "The role of technology in facilitating on-line privacy" (12 May 2000)
- A Workshop on "PET and privacy practice" was held on 5 June 2001 (organised by EICTA)
- A thematic workshop on "Privacy and Identity in information Society" (4/5 October 2001).
  The latter concerns the development and animation of the **e-Forum on Privacy in Information Society** (eprivacy.jrc.it) to become a portal for technical awareness activities that would also promote the exchange of experiences and consolidation of best practice on the deployment of privacy enhancing technologies.
- A meeting of the ISTC Working Party on T&C was devoted to "Biometrics & PET" (5 July 2001).

1.5.4. Standardisation

The Initiative for Privacy Standardization in Europe (IPSE), under CEN (Centre européen de normalisation) / ISSS (Information Society System Standardisation), has been seeking to produce a report on the potential role of standardization in supporting the implementation of Directive 95/46/EC. The work has been mandated and supported by the European Commission.

---

[24] WP 29 (5009/00) Opinion 2/2000 concerning the general review of the telecommunications legal framework, adopted on 3.2.2000, Doc. 5009/00, adopted on 3.2.2000.
WP 36 (5042/00) Opinion 7/2000 on the European Commission Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector of 12 July 2000 – COM(2000)385, adopted on 2.11.2000 (see also part I .3– summary of the main issues addresed in 2000).

In order to carry out the activity, CEN established a broadly representative Steering Group of interested parties, including industry (both as vendors of and as end-users of solutions), consumers, data protection authorities, standards organizations, etc. The Steering Group has been supported by a small Expert Team, whose task it has been to prepare sucessive drafts of the report for discussion and approval by the Steering Group.

Following the European Commission's mandate to CEN to explore the possibilities and need for standardisation in support of the implementation of the European Union data protection directive, the Open Seminar "Standardization - A business tool for Data Privacy" took place in Brussels, on the 23 and 24 March 2000. Representatives of data protection authorities as well as Director General John F. Mogg, European Commission, Directorate General Internal Market, contributed by explaining their respective views concerning the need for standardisation, in particular at international level and on privacy enhancing technologies.

With a view to identifying specific topics suitable for action, the Initiative on Privacy in Standardisation in Europe (IPSE) Steering Group was set up and met three times in 2000. It was decided to set up the CEN/ISSS Project Team, with the task of Drafting the IPSE Report. An Open call for experts in the area of Privacy and Data Protection was therefore made - with closing date on the 26 May 2000 - and a project Team was set up. The kick-off meeting of the Project Team took place on the 10 and 11 October. During this meeting, a discussion on the report's scope, structure and contents took place, and a first timescale has been proposed.

Following the meeting, the IPSE Steering Group worked to define the scope of the report, and appointed the Expert Team. The first draft of the Expert Team's report will be issued for public consultation in 2001.[25]

1.5.5. Third Pillar

Common secretariat

On 17 October 2000, the Council adopted a Decision on the establishment of a Secretariat for the Joint Supervisory Data Protection Bodies set up by the Convention on the Establishment of a European Police Office (Europol Convention), the Convention on the Use of Information Technology for Customs Purposes and the Convention implementing the Schengen Agreement on the gradual abolition of checks at the common borders (Schengen Convention)[26].

This Decision sets up a single, independent data protection secretariat, which would be bound by the above-mentioned Conventions in the exercise of its tasks.

---

25 Draft IPSE report from CEN/ISSS on privacy standardisation. http://www.cenorm.be/isss/Projects/DataProtection/IPSE/IPSE-ET%20DraftFinalReportv05.pdf.

26 Official Journal, L 271 , 24/10/2000 p. 1 – 3.

Eurodac

On 11 December 2000, the Council adopted the EC Regulation (EC) concerning the establishment of "Eurodac" for the comparison of fingerprints for the effective application of the Dublin Convention[27].

The Eurodac system enables Member States to identify asylum-seekers and persons who have crossed an external frontier of the Community in an irregular manner. By comparing fingerprints Member States can determine whether an asylum-seeker or a foreign national found illegally present within a Member State has previously claimed asylum in another Member State.

Eurodac consists of a Central Unit within the Commission equipped with a computerized central database for comparing the fingerprints of asylum applicants and a system for electronic data transmission between Member States and the database. In addition to fingerprints, data sent by Member States will include in particular the Member State of origin, the place and date of the asylum application (if applicable), sex and reference number. Data are collected for anyone over 14 years of age and are encoded directly into the database by the Central Unit or the Member State of origin. In the case of asylum-seekers, data are kept for 10 years unless the individual obtains citizenship in one of the Member States. Data relating to foreign nationals apprehended when attempting to cross an external border illegally are kept for two years from the date on which the fingerprints were taken unless the foreign national receives a residence permit or has left the territory of the Member States.

In the case of foreign nationals found illegally present within a Member State, Eurodac makes it possible to check their fingerprints against those in the central database to determine whether the individual had previously lodged an asylum application in another Member State. After the fingerprints have been transmitted for comparison purposes they are not stored by Eurodac.

Member States of origin must ensure that fingerprints are taken lawfully as well as ensuring that all processing operations involving the use, transmission, conservation or erasure of the data itself is lawful.

In addition to the national data protection authorities, an independent joint supervisory authority is set up, consisting of a maximum of two representatives from the supervisory authorities of each Member State. The joint supervisory authority has the task of monitoring the activities of the Central Unit to ensure that the rights of data subjects are not violated and to resolve implementation problems in connection with the operation of Eurodac. Eventually, the joint supervisory authority will be replaced by the independent supervisory body under Article 286(2) of the EC Treaty and Regulation 45/2001/EC[28].

---

27 Official Journal L 316 , 15/12/2000 P. 1 – 10.

28 See chapter 1.5.1 Data Protection in Community Institutions and bodies.

Europol

On 27 March 2000, the Council of the European Union adopted a decision authorising the Director of Europol to enter into negotiations on agreements with third member States and non-European Union related bodies[29].

According to this Decision, the Director of Europol may only enter into negotiations concerning the transmission of personal data once the Council is satisfied that there are no obstacles to the start of such negotiations, taking account of the laws and administrative practice in the field of data protection in the third State or non-European Union-related body concerned. This Decision authorises the Director of Europol to enter into negotiations with a first group of third States and non-European Bodies : Bolivia, Bulgaria, Canada, Columbia, Cyprus, Czech Republic, Estonia, Hungary, Iceland, Latvia, Lithuania, Malta, Morocco, Norway, Peru, Poland, Romania, Russian Federation, Slovakia, Slovenia, Switzerland, Turkey, United States of America., ICPO-Interpol, UNDCP (United Nations Drugs Control Programme), World Customs Organisation.

Two declarations of the Council were also published with the Decision of the Council in the Official Journal. The first one concerns the relations between Europol and third States and non-European Union-related bodies. The Council states that it shall take into account the law and administrative practice of relevant third States and non-European Union-related bodies in the field of data protection in reaching its decision to authorise the Director of Europol to enter into formal negotiations on agreements providing for the transmission by Europol of personal data. In order to allow the Council to duly consider whether there are any obstacles to the start of such negotiations, it invites Europol to prepare and submit reports to the Council on the laws and administrative practice in the field of data protection in these third States and non-European Union-related bodies. The Council invites the Commission to assist in the preparation of these reports through providing any relevant information in its possession.

The second one concerns the priority to be given to third States and non-European Union-related bodies where the Council states that priority should be given to the accession candidates, the Schengen cooperation partners (Iceland and Norway), Switzerland and Interpol.

Eurojust

The European Council summit in Nice on 9 December 2000 agreed upon further steps for Eurojust in order to enhance judicial co-operation in criminal matters (see Article 31 of the Treaty of Nice). It should be composed of national prosecutors, magistrates, or police officers of equivalent competence, detached from each Member State according to its legal system.

29 Official Journal C 106, 13.04.2000.

2. THE COUNCIL OF EUROPE[30]

The Council of Europe continued the work that it regularly carries out on the issue of data protection.

The consultative committee (T-PD) of the Convention for the protection of Individuals with regard to automatic processing of personal data (EST 108) adopted the draft Additional Protocol to Convention ETS No 108 on supervisory authorities and transborder data flows on 8 June 2000. The text has been subsequently submitted to the Committee of Ministers for adoption and opening to signature by parties to the Convention.

The project group on data protection (CJ-PD) adopted on 13 October 2000 a Draft Recommendation on the protection of personal data collected and processed for insurance purposes, and its Explanatory Memorandum. Both texts were transmitted to the European Committee on Legal Co-operation (CD-CJ) for approval. The Article 29 Data Protection Working Party adopted an opinion for the attention of the CD-CJ and the Committee of Experts on Crime in Cyber-space (PC-CY) concerning the draft Convention on Cyber-crime being prepared at the latter Committee. It further examined a report on video surveillance prepared by Mr Giovanni BUTTARELLI and considered follow-up action to this report.

The Community, represented by the Commission, intervenes within both the T-PD and the CJ-PD when the items under discussion fall within the external competencies resulting from Directives 95/46/EC and 97/66/EC. This was the case for the texts referred to above. This co-operation with the Council of Europe aims to ensure full compatibility with Community directives.

3. PRINCIPAL DEVELOPMENTS IN THIRD COUNTRIES

3.1. European Economic Area

3.1.1. Iceland

The directive 95/46/EC was implemented in Iceland in the year 2000 with the Act on Protection of Individuals with regard to the Processing of Personal Data No. 77/2000. It was enacted on 23 May 2000 and entered into full force on 1 January 2001. The Act implements the directive in full and replaces older legislation on the subject. The first Icelandic Act on the processing of personal information was passed in the year 1981. The Act No. 77/2000 provides for a new, independent government Agency to be formed, the Data Protection Authority (Personuvernd). Personuvernd has a five member board, chaired by professor Pall Hreinsson. Under the Act, Personuvernd took over the responsibilities of the former Data Protection Commission, a committee appointed by the Minister of Justice. Personuvernd is run by a Commissioner who is appointed for four years at a time. Personuvernd's first Commissioner, Mrs. Sigrun

[30] http://stars.coe.fr/index_e.htm

Johannesdottir, was appointed on 18 July 2000 for a tenure that began on 1 August 2000.

Various legislative measures, taken in Iceland the year 2000, had an impact on privacy and data protection. The principal legal acts in this category are:

- Act on the Participation of Iceland in the Schengen-cooperation No.15/2000 and Act on the Schengen Information System No 16/2000. According tothe legislation, Personuvernd shall monitor the adoption of the informationsystem in Iceland to ensure that the rights of those registered will beprotected.
- Act on Doorstep and Remote Selling Contracts No. 46/2000. In Art. 14 of the Act, rights of the recipients of direct marketing are stipulated, among them the right to opt-out via a public registry.
- Act on Biobanks No. 110/2000. The Act introduces a legal framework for the building and running of biobanks, i.e. companies and institutions that store biological samples obtained from human beings. According to the Act, Personuvernd shall define the criteria that the biobanks will need to meet regarding the security of personal data and their processing.

3.1.2. Norway

The Norwegian Data Inspectorate was set up in 1980 and was until January 1st to ensure enforcement of the Act relating to personal Data registers of 1978.
After January 1st the new Act; the Personal Data Act (Act of 14th april 2000 no 13 relating to processing of personal data) will be enforced.
The purpose of this Act is to protect natural persons from violation of their right to privacy through processing of personal data. The act shall help to ensure that personal data are processed in accordance with fundamental respect for the right to privacy.

The Norwegian Data Inspectorate is an independent administrative body, and from January 1st 2001 under the Ministry of labour and government administration. The Inspectorate was earlier under the Ministry of Justice.

The Personal Data Act has raised new issues for the Data Inspectorate.
The Inspectorate is no longer required to deal with applications for licences, but use resources to ensure that laws and regulations are complied with and to provide information concerning the protection of privacy and data security.

The Norwegian Data Protection Act emphasises the individual's right to control the processing of his/her personal data through an extensive use of a formal consent from the data subject. This principle also evolves into fundamental rights for the data subjects, such as giving access to information concerning him- /herself and information about the data processing and the right to correction and deletion of data incorrect and excessive information.

The Norwegian Data Protection authority carried out a total of 19 inspections. A major intention behind the Act is to increase the amount of inspections. This will require more resources and an organisation with a focus on faster results.

The Personal Data Act has given the Privacy Appeals Board the right to decide appeals against the decisions of the Inspectorate. The Board is an independent administrative body subordinate to the King and the Ministry and consists of seven members. The board has dealt with only one appeal so far.

It is of great importance for The Inspectorate to ensure that both the controller and the processer, by means of planned, systematic measures, ensure satisfactory data security with regard to confidentiality, integrity and accessibility in connection with the processing of personal data.

The work with Public Relations is important for reaching out to the public with information about rights and duties. The Inspectorate use several means to reach out, for instance conferences, press releases, and web-information such as FAQs and newsletters.

3.2. Candidate Countries

For all the applicant countries, the reinforced pre-accession strategy aims at allowing their integration of the Community 'acquis'. In this spirit, the accent is put both on the adoption of legislation, in particular Directive 95/46/CE, and on the establishment of the administrative structures necessary for its effective implementation, such as independent data protection supervisory authorities.

Developments in these field have taken place in a number of applicant countries. New general legislation was adopted by Latvia in March, by the Czech Republic in June and by Lithuania in July, aiming at implementing the community acquis and in particular Directive 95/46/EC, while Slovenia adopted specific legislation in the field of health data. Convention 108 of the Council of Europe was signed by Estonia, Lithuania, Slovakia, the Czech Republic and Latvia, and it was ratified by Slovakia.

3.3. United States of America

The Article 29 Data Protection Working Party examined the documents resulting from the discussions between the European Commission and the US Department of Commerce in its February, March, May, June and July meetings.

In February the Article 29 Data Protection Working Party expressed the opinion that a number of fundamental issues had to be addressed before a finding on adequacy could be made. In particular, the outstanding issues discussed concerned the effectiveness of the proposed enforcement mechanisms and the role of the FTC in this area and a discussion of the text of the FAQ's. The Article 29 Data Protection Working Party expressed nevertheless its continued support for the discussions, welcoming the improvements in the texts submitted by the U.S. government.

During the March meeting the Article 29 Data Protection Working Party continued to discuss the substance of the arrangement and assist the European Commission in its dialogue with the U.S. by highlighting areas of concern and adopted Opinion 3/2000. At the May meeting another opinion was discussed and adopted (Opinion 4/2000) The

general consensus was that although some reservations about the level of protection afforded by the arrangement persisted, the Article 29 Data Protection Working Party recognised that some compromises had to be made to secure a working arrangement and that there would always be the opportunity to check how the system was working in practice once it was introduced.

By the July meeting the Article 29 Data Protection Working Party considered the exact legal basis on which the Safe Harbour Arrangement was to be adopted and discussed the reservations expressed in the European Parliament resolution on the matter. In October, the Article 29 Data Protection Working Party discussed the internal working procedures of the Data Protection Authority Panel (which operates as an enforcement mechanisms for organisations in the Safe Harbor). The final document was adopted in the November meeting. The Article 29 Data Protection Working Party did, however, expressly reserve the right to revisit issues discussed in their opinions at a later date in the light of experience.

3.4. Other third countries

3.4.1. Australia

In June 2000 the Commission presented a submission to the Australian Government on their Privacy Amendment Private Sector Bill 2000 stating that the law as it currently stood could not be found to be adequate under Directive 95/46/EC. In response, the Australians issued a report making 23 recommendations aimed at strengthening the protection afforded by the Bill.

In its meeting held on 13 July 2000 the Article 29 Data Protection Working Party discussed this issue and were in agreement with the Commission that the Bill did not go far enough in protecting privacy rights. The Article 29 Data Protection Working Party expressed the hope that they could have a constructive input into the discussions between the European Commission and the Australian Government regarding the Bill and in its meeting in October 2000 decided to adopt an opinion on this issue in the near future.

3.4.2. Canada

During the course of the meeting of the Article 29 Data Protection Working Party held in May 2000, a copy of the Canadian Personal Information Protection and Electronic Documents Act which was adopted in Canada the previous month was distributed amongst the members in order that they could examine same with a view to adopting a Article 29 Data Protection Working Party Opinion on its adequacy.

In its meeting in October 2000, the members having had the opportunity to review the legislation discussed the matter and agreed that the critical points concerned sensitive data and public data. The Article 29 Data Protection Working Party agreed in principle to preparing an opinion on the matter in the following months.

3.4.3. Jersey, Guernsey and the Isle of Man

Following the presentation of a preliminary analysis on these Territories in February, and a letter by the British Commissioner, the Chairman of the Article 29 Data Protection Working Party sent letters to the data protection supervisory authorities of each of the Dependencies in November, in order to ask for clarification on several problematic points.

4. OTHER DEVELOPMENTS AT INTERNATIONAL LEVEL

4.1. Organisation for Economic Co-operation and Development (OECD)[31]

The OECD Working Party on Information Security and Privacy (WPISP) promotes an internationally coordinated approach to policymaking in security and protection of privacy and personal data in order to help build trust in the global information society and facilitate electronic commerce. One important element for global networks to be trustworthy is that personal data must be effectively protected.

Following the work of this group, a Report on transborder data flow contracts in the wider framework of mechanisms for privacy protection on global networks was declassified. Further, the Online Privacy Policy Statement Generator was declassified and made available online on the OECD Web site, as an online tool intended to help Webmasters and administrators to create their own privacy policy statement to be posted on their Web site. The OECD, in co-operation with the Hague Conference on Private International Law and the International Chamber of Commerce organised a Joint Conference on Alternative Dispute Resolution in the Online Environment, as a first step to help ensure that effective enforcement mechanisms are available both to address non-compliance with privacy principles and policies and to ensure access to redress.

[31] http://www.oecd.org/EN/home/0,,EN-home-0-nodirectorate-no-no-no-0,FF.html